



First Access

OPERATOR GUIDE

February 2024

Table of Contents

Introduction.....	4
First Access Application Overview.....	5
Typical First Access Configuration	6
• Single Server – Single Client	6
• Single Server – Multiple Clients	6
PC & Network Requirements	7
Step 1. Software Installation	7
• Server & Client	9
• Client Only	9
Step 2. Software Configuration	11
• Host Server Name or IP Address & REST API Key	12
• Credential Enroller	13
• History Retention	14
• DST (Daylight Saving time)	14
• Display Format	15
• Email Settings	16
• Alarm Holiday Schedule	16
• Active Directory Import	17
• Active Directory Account Service	18
• Active Directory Access Service	19
Step 3. Panel and Reader Definition.....	21
• Add Panel	21
• Add Reader	22
• Define Auxiliary Input Point	29
• Define Auxiliary Output Point	30
• Edit and Delete Panel	31
• Reader Status	31
• Reader Commands, Scheduled Commands, Triggers, Counters	32
• Reader Events	46
• Alarm Notifications	49
• Alarm Queue	55
• Application Windows	56
• Input and Output Commands	56
Step 4. Schedules, Profiles, Users and Operators	58
• Access Schedules	58
• Unlock Schedules	59
• Shunt Schedules	61
• Output Schedules	62
• Holiday Schedules	63
• Access Profiles	64

• Add Cardholders and Card Groups.....	66
• Search, Edit and Delete Cardholder	72
• Operator Profiles	76
• Cardholder and Credential Report	78
Step 5. History and Audit Report.....	79
• History Retention	79
• On-board Audit Event Storage	79
• View Audit History	80
Elevator	82
• Floor Groups, Access Groups and Floor-Unlock Schedule.....	82
• Add Elevator Panel	85
• Manage Elevator Floors.....	86
Software Update & Upgrade.....	89
Appendix.....	91
• Database Backup & Restore Utility	91
• Bulk Credential Load Utility	92
• FA Access View	93
• First Access Import Utility	94
• SQL Server Connection Configuration Utility.....	96
• Email Diagnostics.....	97
• Daily Synchronization	98
Troubleshooting.....	99

CAUTION: EMERGENCY LOCKDOWN

Emergency lockdown functions must operate totally independent of the access control system and must not rely on operation of card readers, access control panels, communications networks, communications devices or host software. Cansec accepts no responsibility for direct or consequential damages resulting from the failure of emergency lockdown functions which are dependant in any way on the operation of card readers, access control panels, communications networks, communications devices or host software.

Copyright © 2024 Cansec Systems, Ltd.

Introduction

First Access software is extremely cost-effective and easy to use to manage the MAP1, MAP2 and MAPMINI door controllers. The MAP2 panel can be provisioned as door controller or as elevator controller. There are two editions of the software **First Access Express** with 4-client concurrent connections, and **First Access Advanced** with 20-client concurrent connections. Both versions support up to 450 controllers and 100,000 users. The final door capacity is dependent on the number and type of controllers. If all MAP1s are used and provisioned for 4 readers then the door count is 1800. If all MAP2s are used and provisioned for 8 readers then the door count is 3600. If only MAPMINIs are used then the door count is 450. The software also supports elevator control using MAP2 controller provisioned as elevator controller. The MAP2 controller can be provisioned as a 16-floor elevator controller. However, with the optional add-on H1000 panels the MAP2 controller can be provisioned to control 32 or 48 or a maximum of 64 floors. The controllers support scheduled commands, triggers, timed anti-passback, local anti-passback, zone anti-passback and double-swipe privilege. It also supports up to 64 bit Wiegand-output reader technologies such as proximity, keypad, and biometric.

All programming changes and commands from the software are instantly transmitted to all door controllers. The controller stores all cardholder data in non-volatile memory to ensure continued operation and security in the event that communication to the host PC is lost. Reader events are automatically transmitted to the PC in real time and stored on the hard drive for viewing and report generation.

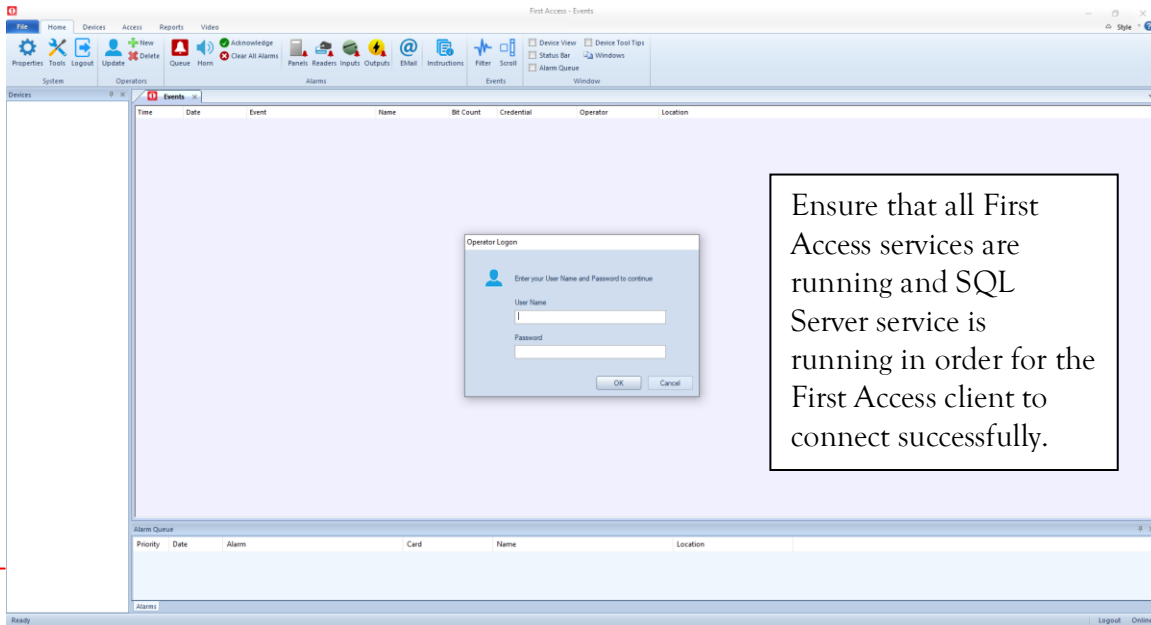
Key Features

- Up to 100,000 cardholder/user capacity
- Up to 1024 reader capacity
- Up to 10 First Access clients
- Controls up to 64-floor elevator
- Real time communications
- Programmable access profiles and holidays
- Built-in Ethernet port for software communication
- Automatic door unlock schedules
- Alarms for forced entry/door held open conditions
- Timed and local anti-passback
- Double-swipe privilege per user per door
- Optional input/output points
- Scheduled commands, customizer modules
- Triggers and counters
- Email notification
- Uses Microsoft SQL database

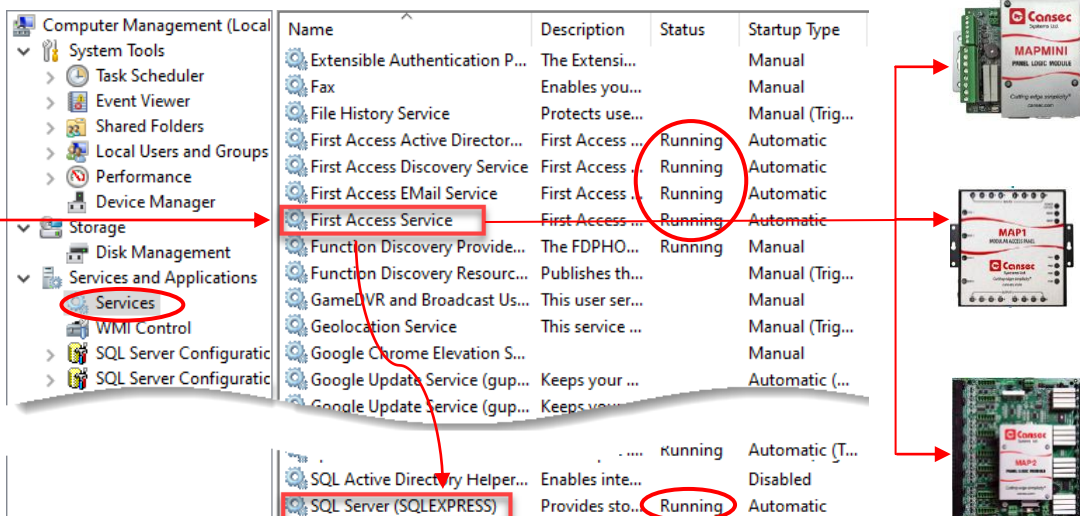
First Access Application Overview

The First Access application comprises of three components: server, client and SQL database. The server, client and SQL database typically run on the same computer.

- First Access Client: A graphical user interface (GUI) that you, one of the operators, use to interact with just the First Access Server only.



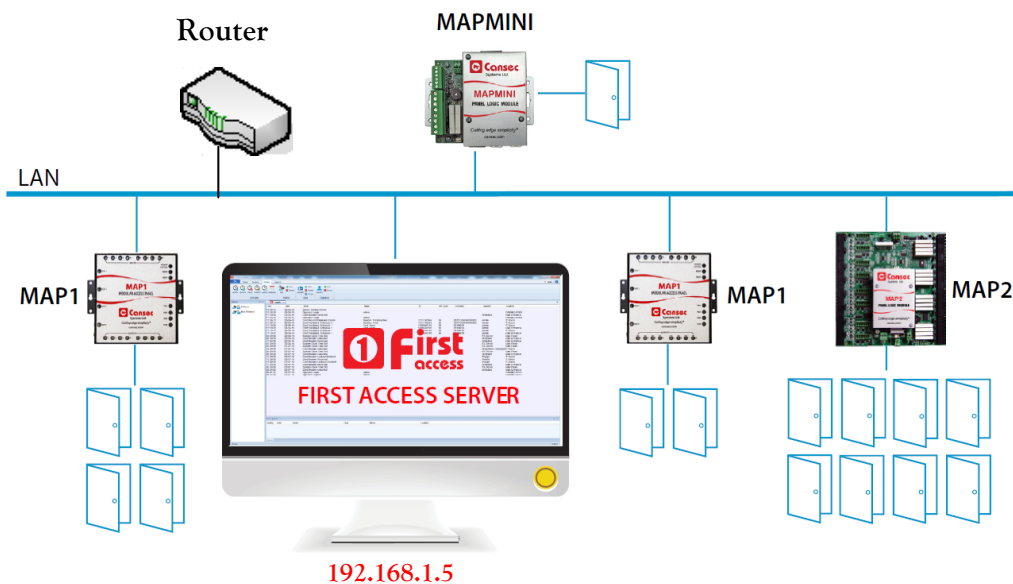
- First Access Server: Runs silently in the background as a Windows Service. It communicates with other First Access services, the controllers, the SQL database and at the same time interacts with the operators via the First Access Client.



Typical First Access Configuration

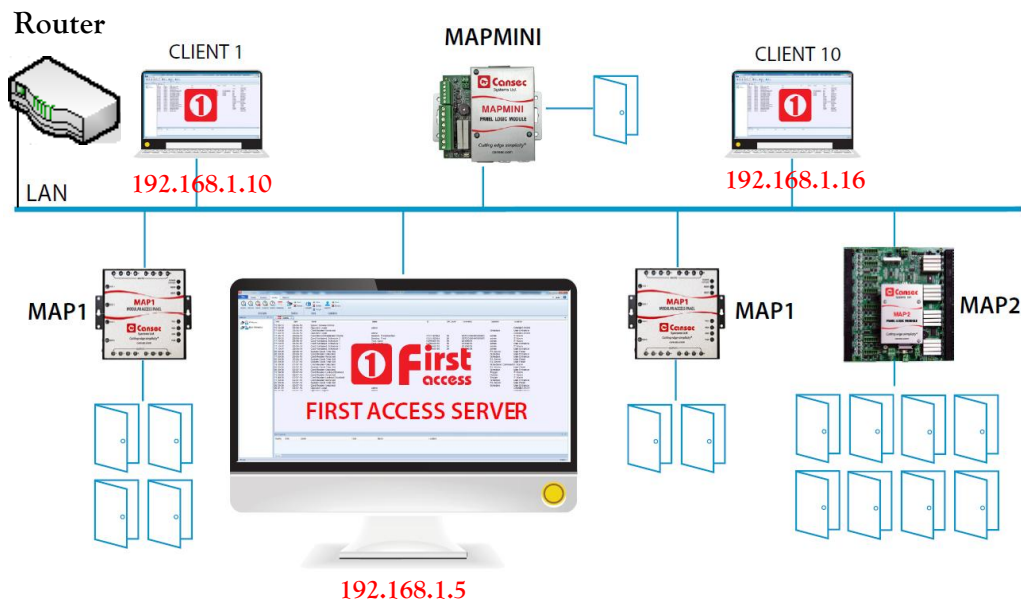
SINGLE SERVER – SINGLE CLIENT

The First Access server and client are installed on the same computer. The client communicates locally with the server only and nothing else. *See application overview.*



SINGLE SERVER – MULTIPLE CLIENTS

The First Access server and client are installed on a dedicated computer. Additional clients are installed on other computers or workstations. Those additional clients communicate via the network interface with the server only and nothing else. *See application overview.*



Firewall must be configured on the server to allow incoming TCP traffics from the clients to reach the server on port 5005. Please consult with your IT personnel for firewall configurations and IP address or host name of the server for the clients to connect to

PC & Network Requirements

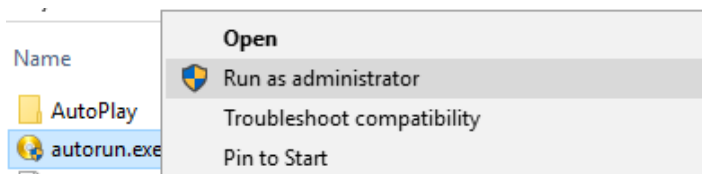
- All 64 bit versions of the following Windows Operating Systems: Windows 10, 11, Windows Server 2008, 2012, 2016 and Windows 2019. All versions must have the latest Windows Updates.
- See Microsoft's web site for CPU, RAM and disk space requirements for the aforementioned operating systems, and for SQL Server requirements:
- USB port and USB thumb drive
- Network cables, router
- Network adapter

Important: Microsoft SQL database must be backed up regularly. See Appendix section for more information.

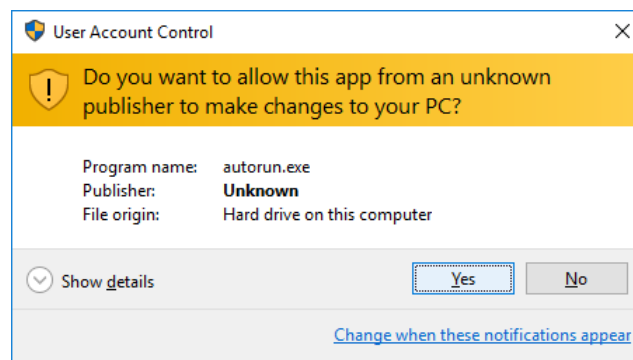
Step 1. Software Installation

Important: *If you require multiple computers, having First Access client installed, to manage the system then consult with your IT personnel to configure a firewall rule on the server computer to allow incoming TCP traffic on port 5005 in order for the First Access clients to communicate with the First Access server. Up to 2 clients are allowed for **First Access Express** and up to 10 clients are allowed for **First Access Advanced**.*

1. Log on to the computer with an administrative account.
2. Download **First Access** software from www.cansec.com/downloads.
3. Unzip and open the folder First Access.
4. Right click on autorun.exe and select Run as administrator.



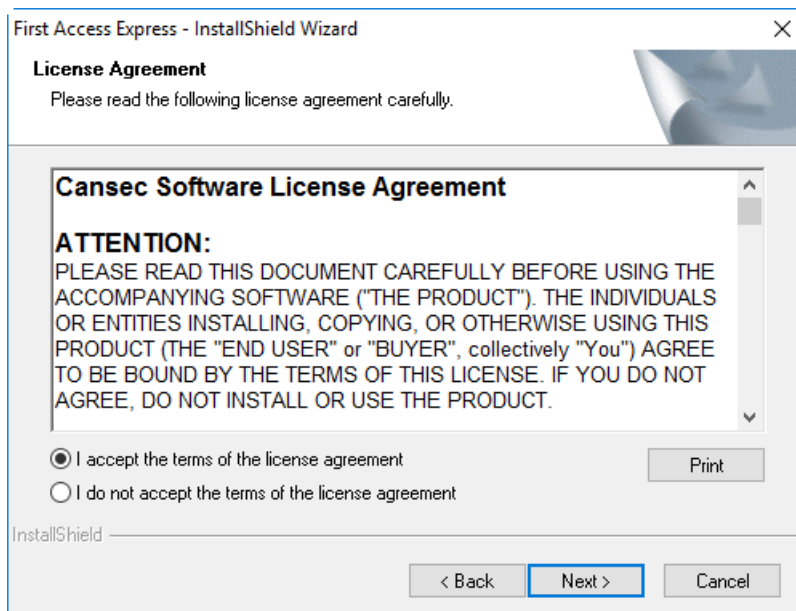
5. When prompted, select **Yes** to continue.



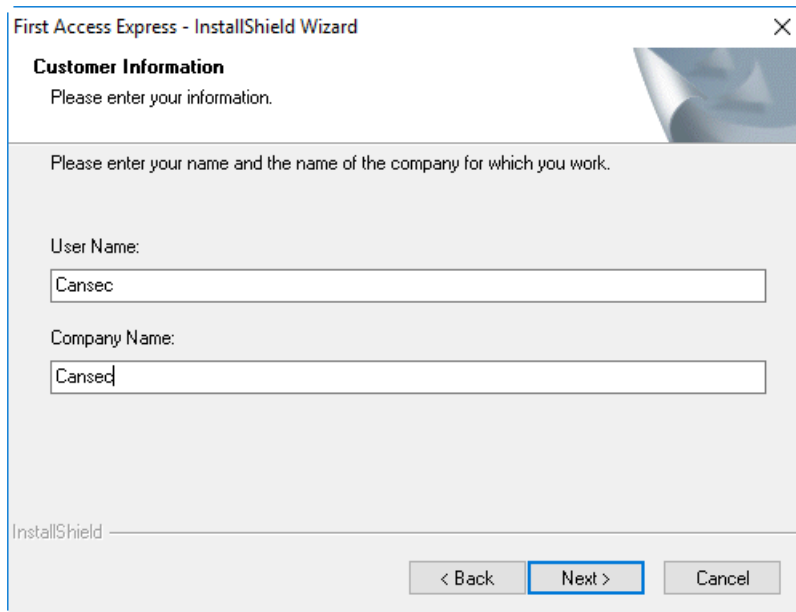
6. If you have purchased the advanced edition then select **Install First Access Advanced**. Otherwise select **Install First Access Express**. When prompted select **Next** to continue.



7. Read and accept the terms of the license agreement then select **Next** to continue. Select **Cancel** otherwise.



8. Enter User Name and Company Name and select **Next** to continue.



First Access Express - InstallShield Wizard

Customer Information
Please enter your information.

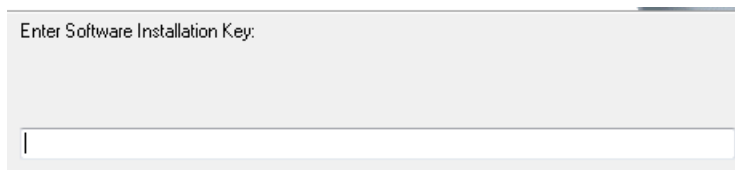
Please enter your name and the name of the company for which you work.

User Name:
Cansec

Company Name:
Cansec

InstallShield

< Back Next > Cancel



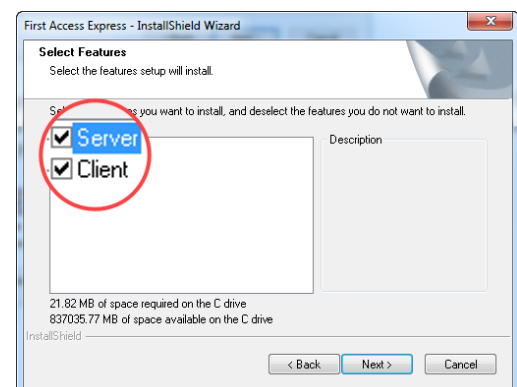
Enter Software Installation Key:

Note: Applicable to *First Access Advanced* only.
Software key must be purchased from a Cansec dealer.

9. Select the features you wish to install and click **Next** to continue.

SERVER & CLIENT

If you wish to install both server and client on the same computer then select both options and click **Next** to continue. This is a typical installation.



First Access Express - InstallShield Wizard

Select Features
Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☒ Server
☒ Client

Description

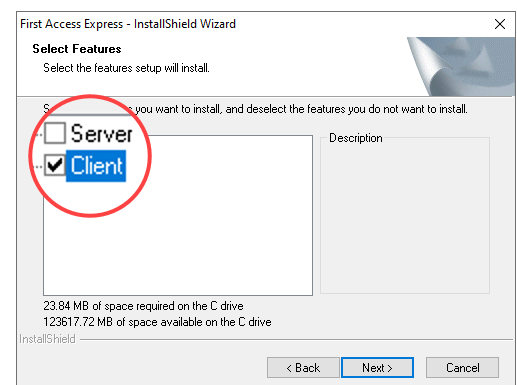
21.82 MB of space required on the C drive
837035.77 MB of space available on the C drive

InstallShield

< Back Next > Cancel

CLIENT ONLY

If you wish to manage the First Access system from multiple computers then first install the server and client on a dedicated computer. Next use the same installation package to install clients on other workstations but select just the Client only. Consult with your IT Personnel to configure a firewall rule on the server computer to allow incoming TCP traffic on port 5005 in order for the First Access clients to communicate with the First Access server.



First Access Express - InstallShield Wizard

Select Features
Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☐ Server
☒ Client

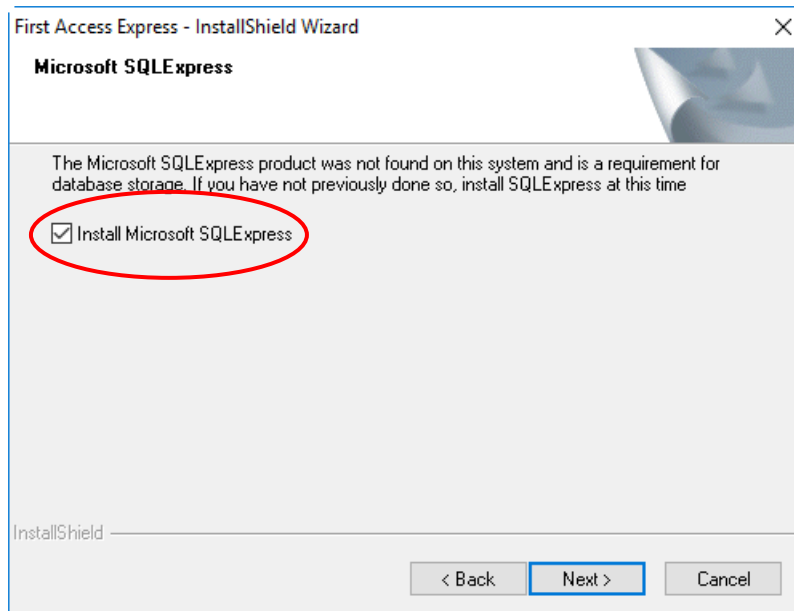
Description

23.84 MB of space required on the C drive
123617.72 MB of space available on the C drive

InstallShield

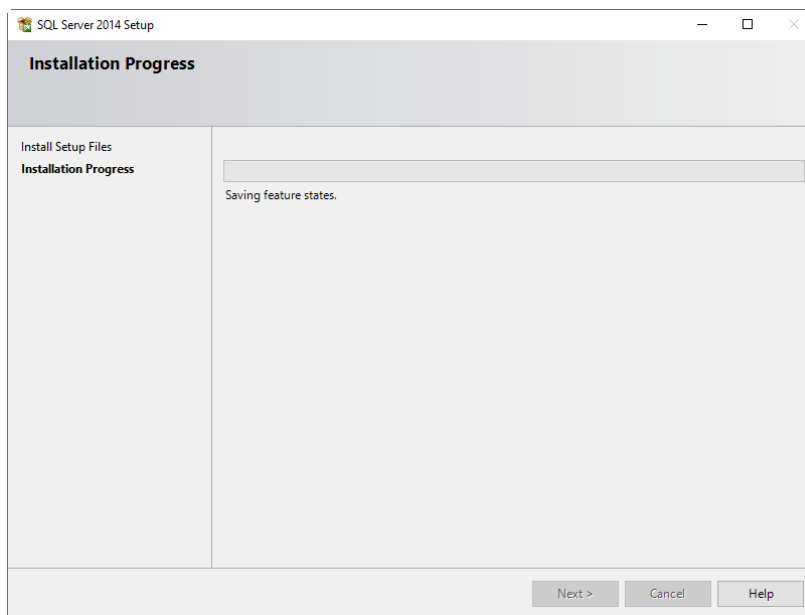
< Back Next > Cancel

10. If SQL Express is not installed on this computer, you will be prompted to install it. Select **Next** to continue. **Important:** SQL installation may fail if Windows Operating System does not have the latest windows updates.

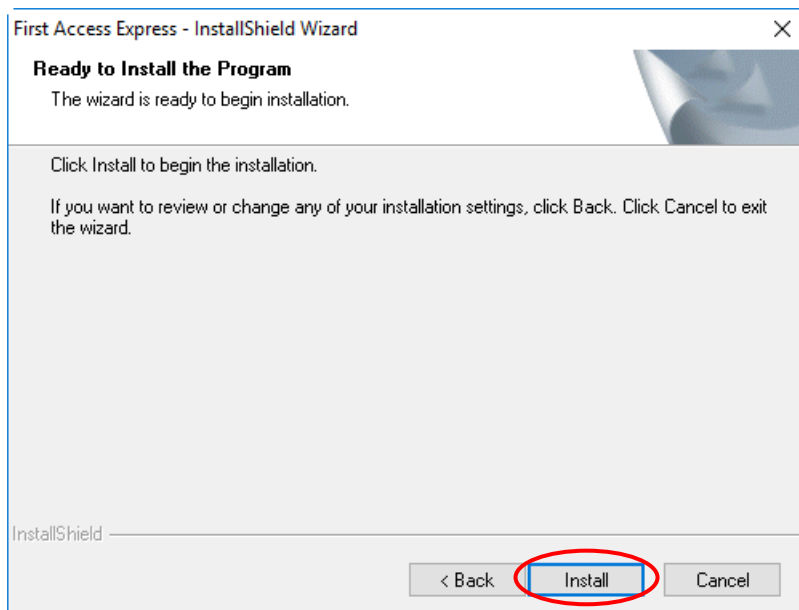


Note: *If you wish to use your own SQL server elsewhere then unselect **Install Microsoft SQL Express**. Select **Next** to skip Microsoft SQL Express.*

11. Wait for the SQL Express Installation to complete.



12. After SQL installation has finished select **Install** to install First Access software, and at the end of the process select **Finish** to complete the installation.



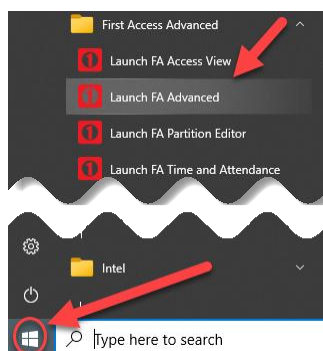
13. Select the X button on the top right corner to exit the Auto Play Installation Package.



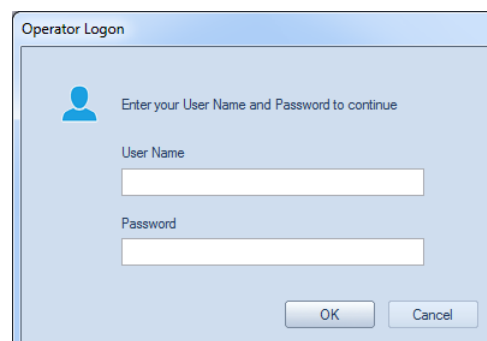
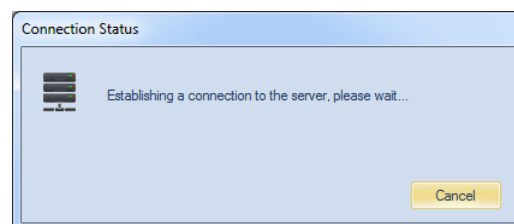
Step 2. Software Configuration

This section describes the initial steps to configure the First Access system. These steps are typically done by the installation company or the system administrator.

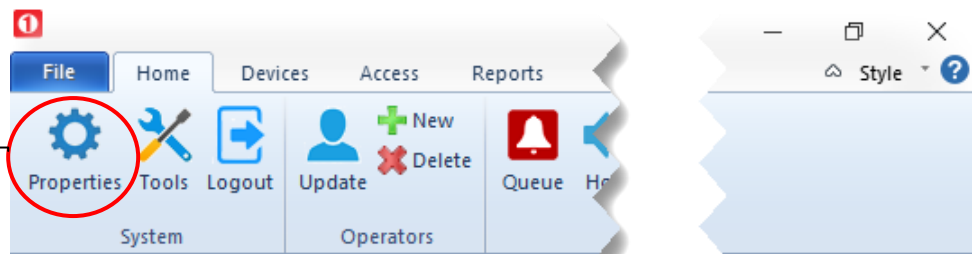
1. Launch First Access software from the shortcut on the desktop or from the Start menu of Windows.



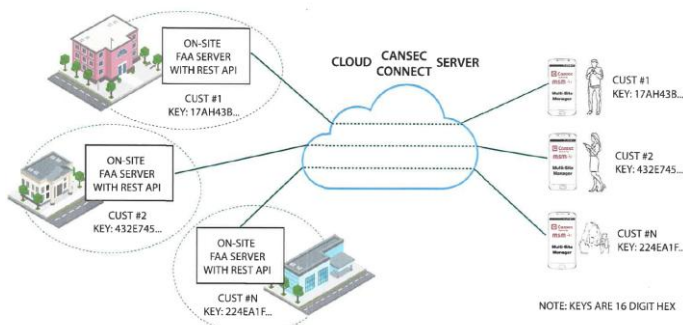
2. Use the default **admin** for both User Name and Password to log on. You may be prompted to change the default password.



HOST SERVER NAME OR IP ADDRESS & REST API KEY



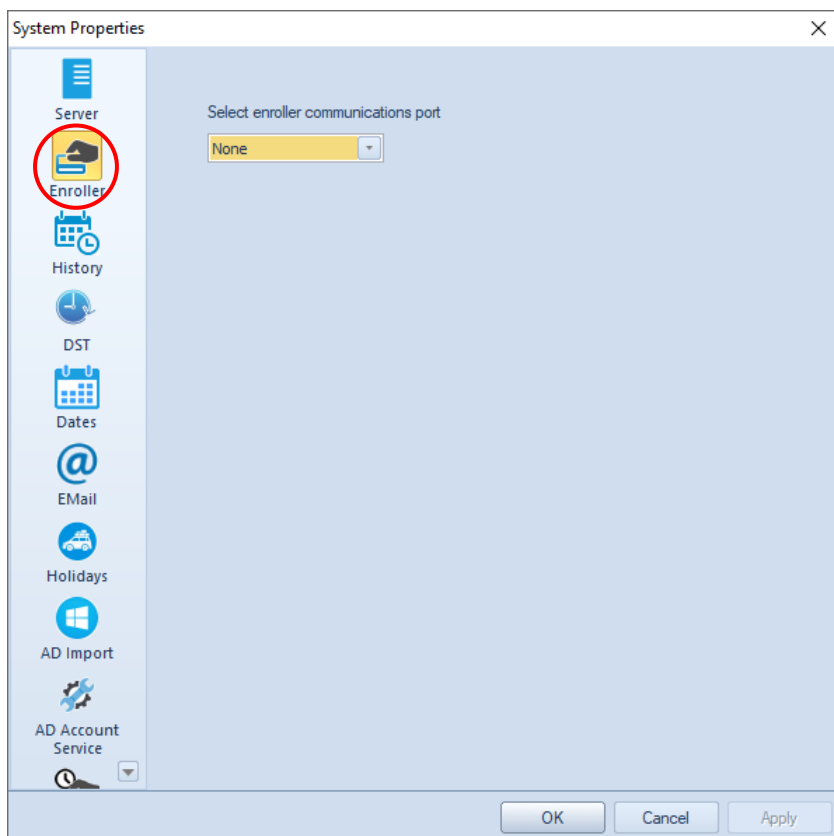
Normally First Access Server and the First Access Client are installed on the same computer so the default settings should be: IP Address **127.0.0.1** and Port **5005**.



FA Connect API Key or REST API Key allows your First Access Advanced Server to communicate with the Cansec Connect Server which facilitates the connection between your First Access Advanced Server and the Cansec MSM app on your phone

CREDENTIAL ENROLLER

If a credential enroller is purchased and used, select the communication port number to which it is connected. Otherwise skip this step.

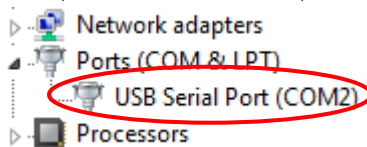


Note: The communication port can be found in Windows' Device Manager. See example below showing COM2. Select **None** if no card enroller is used.

Credential Enroller
(USB Cable)

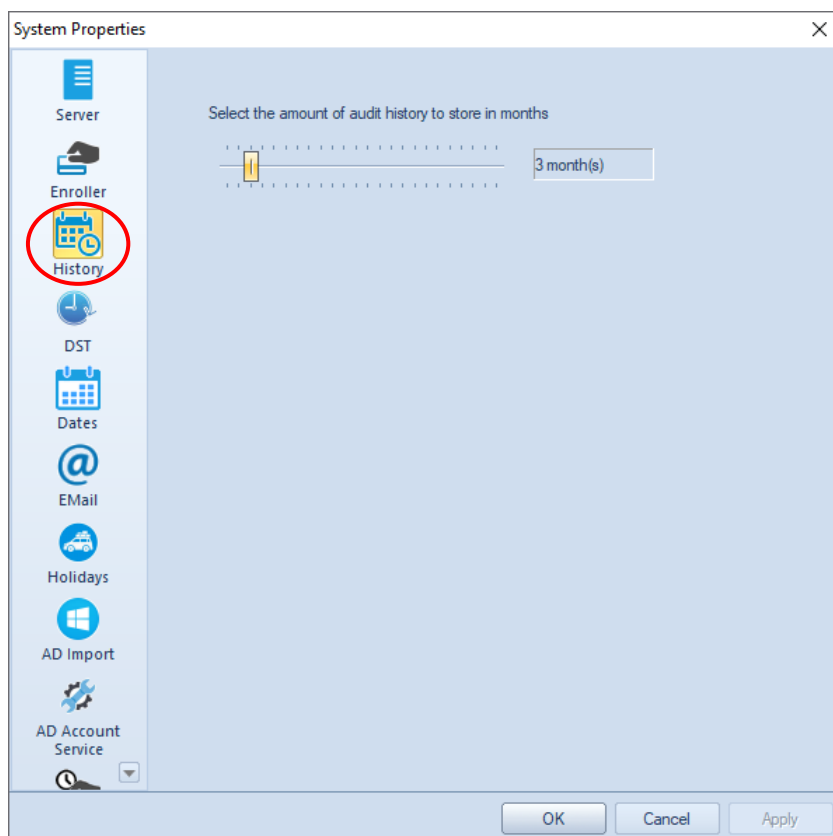


Communication Port
(USB Serial Port)



HISTORY RETENTION

First Access is a real-time system. The events are constantly being recorded in the Microsoft SQL Database stored on the computer's hard drive. Use the slider to select the duration, in months, the audit history is to be retained. Audit history older than the specified number of months will be purged automatically.



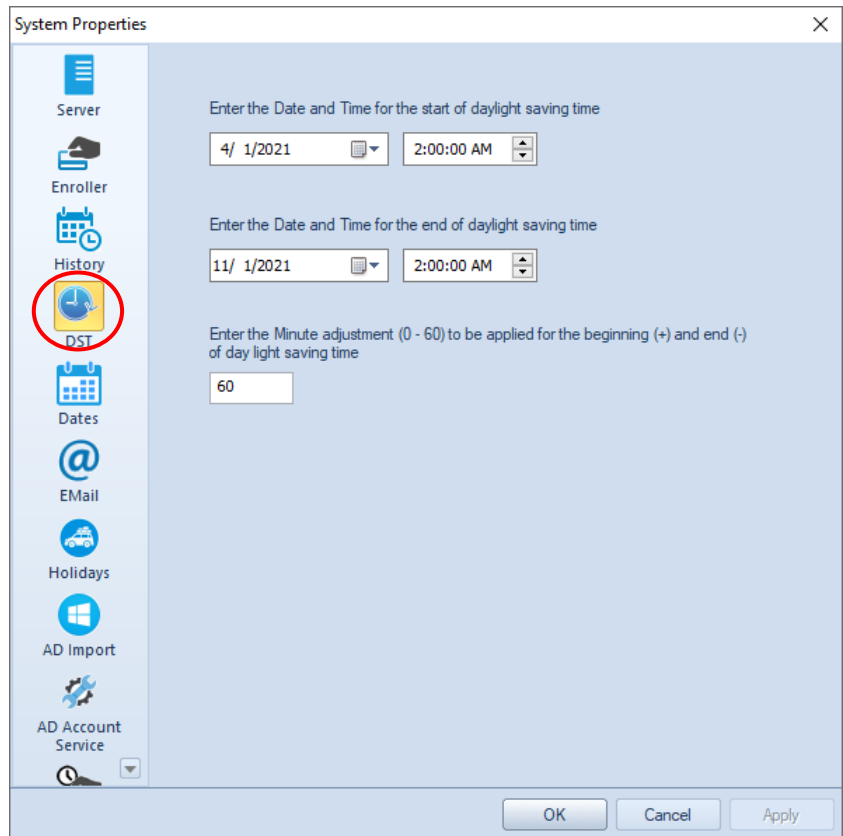
DST (DAYLIGHT SAVING TIME)

Daylight Saving Time may be required in certain region. Select the date and time when daylight saving time starts and ends. Specify the minutes of adjustment.

Example: See image on next page

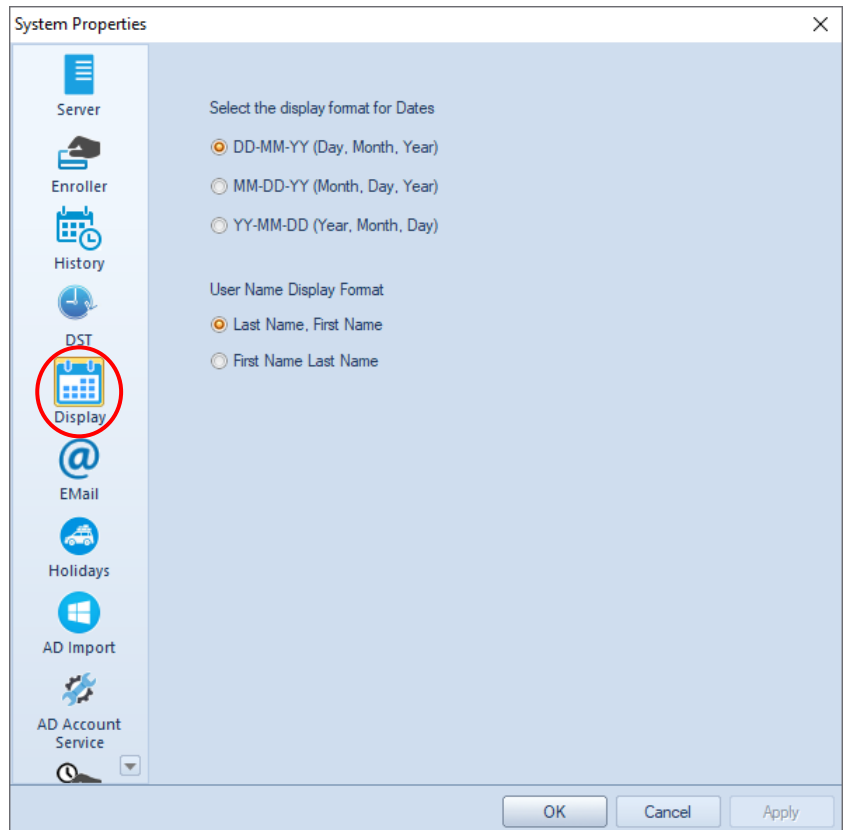
- DST starts on March 11, 2018 at 2AM and the clock on the control panel will be turned forward 60 minutes.
- DST ends on November 4, 2018 at 2AM and the clock on the control panel will be turned backward 60 minutes.
- All onboard schedules e.g. access schedules, unlock schedules etc... will be changed accordingly by DST adjustment.

Note: In addition to the DST settings, the First Access Server software uses the clock from the computer to automatically synchronize the clocks of all the controllers. The synchronization occurs daily at 3:00 AM to ensure that the clocks of all controllers are updated accordingly even if DST is not configured on each panel.



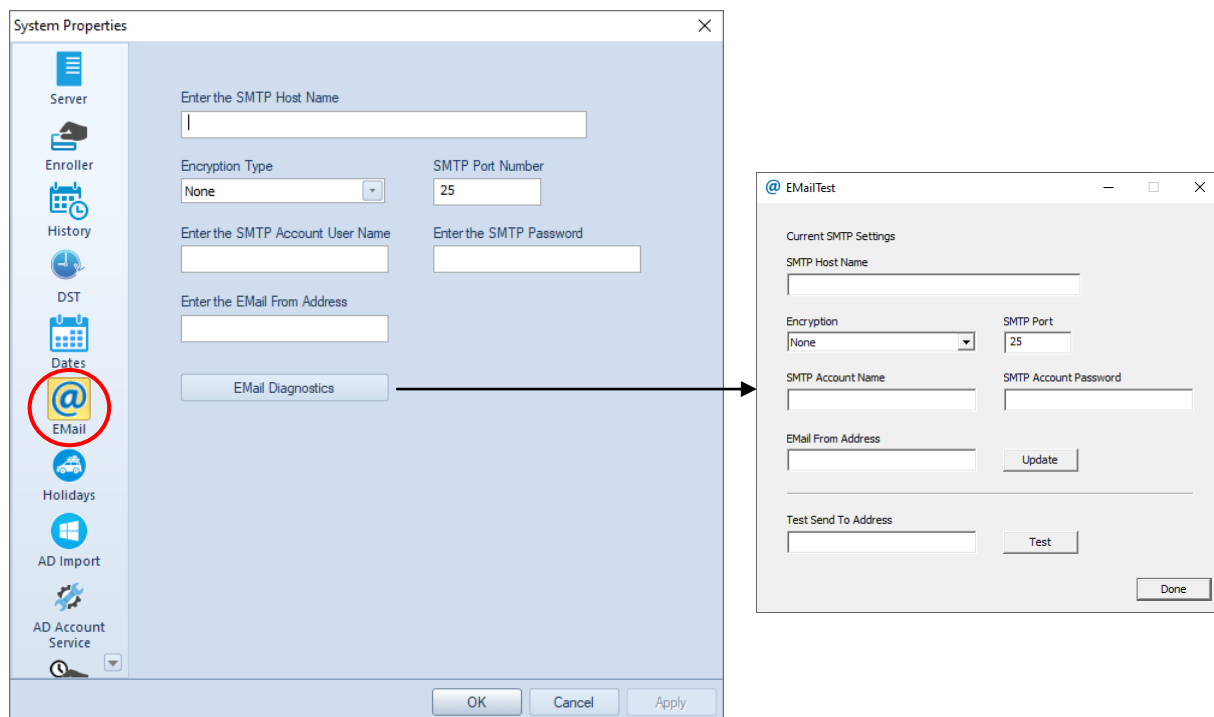
DISPLAY FORMAT

Select desired display format for the dates and the user names



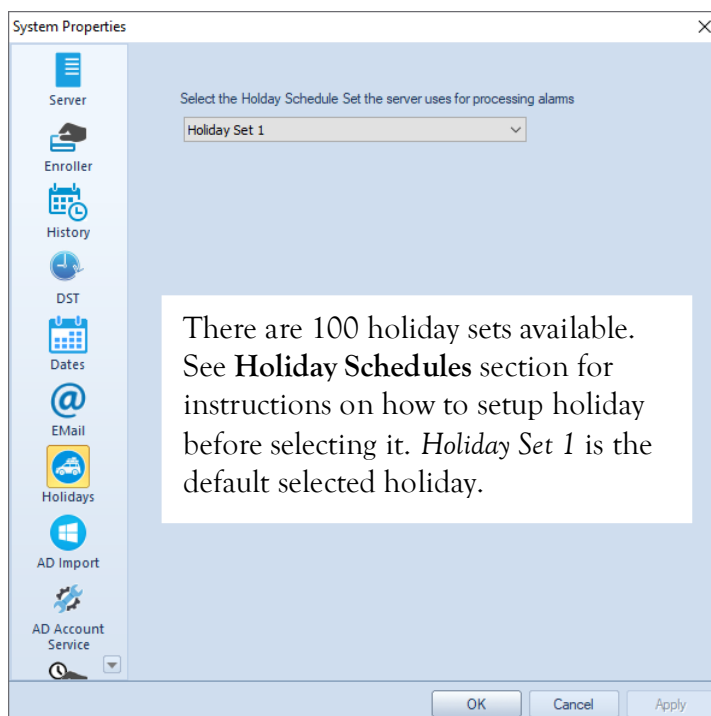
EMAIL SETTINGS

Email notification feature is available in **First Access Advanced** only. For email setup, contact IT personnel or email administrator for required information to enter in the email setup screen.



ALARM HOLIDAY SCHEDULE

Alarm holiday schedules are available in **First Access Advanced** only. They are used to determine when not to process alarms.

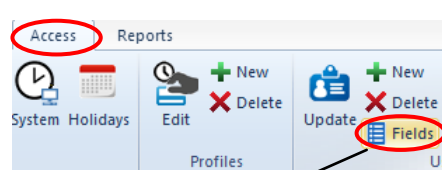
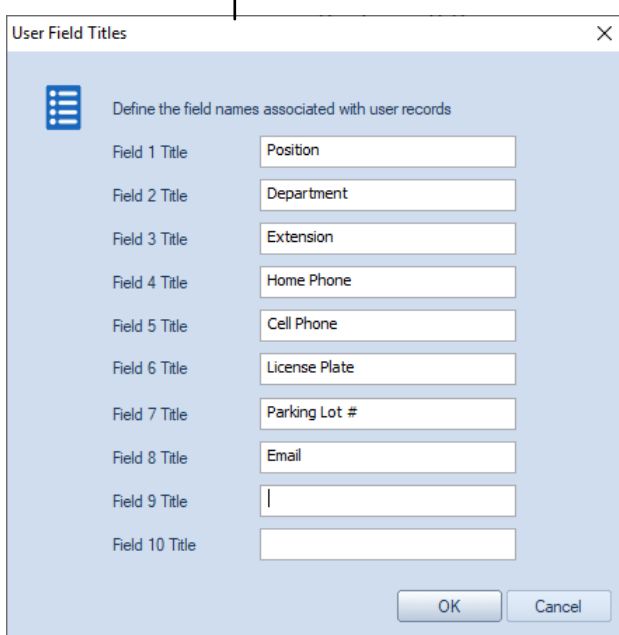
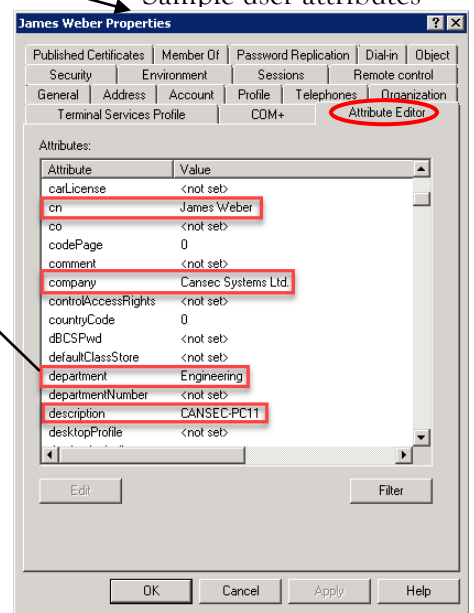
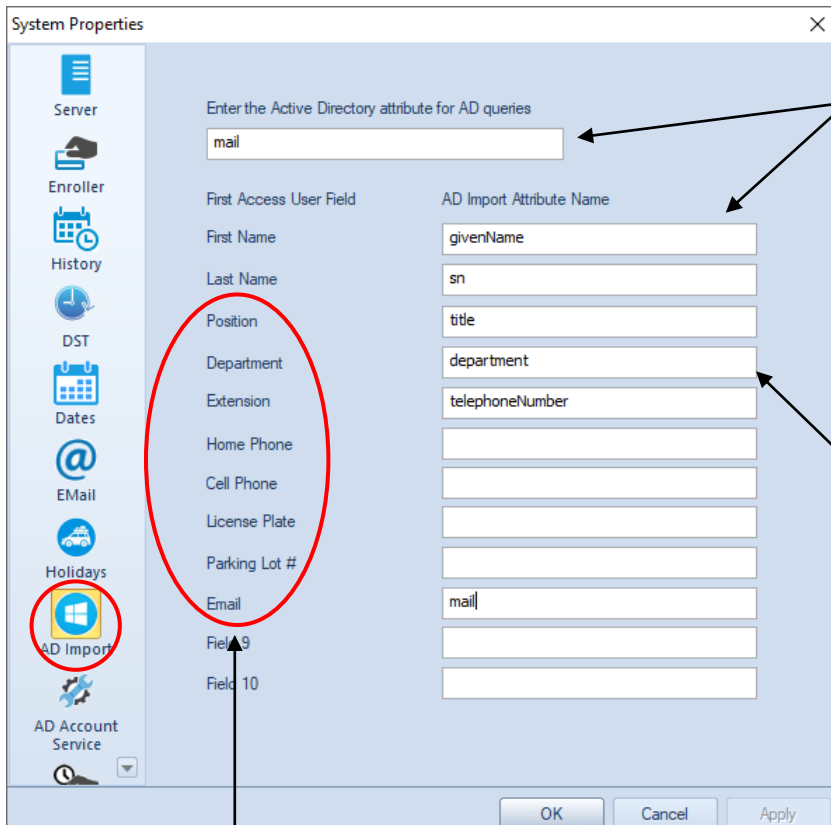


ACTIVE DIRECTORY IMPORT

Active Directory (AD) Import is available in **First Access Advanced** only. This feature helps importing the name and other attributes of users from Active Directory into First Access. All attributes must first be setup by the IT personnel. Active Directory Attributes below could be obtained from IT personnel.

All attributes must first be setup up by IT personnel.

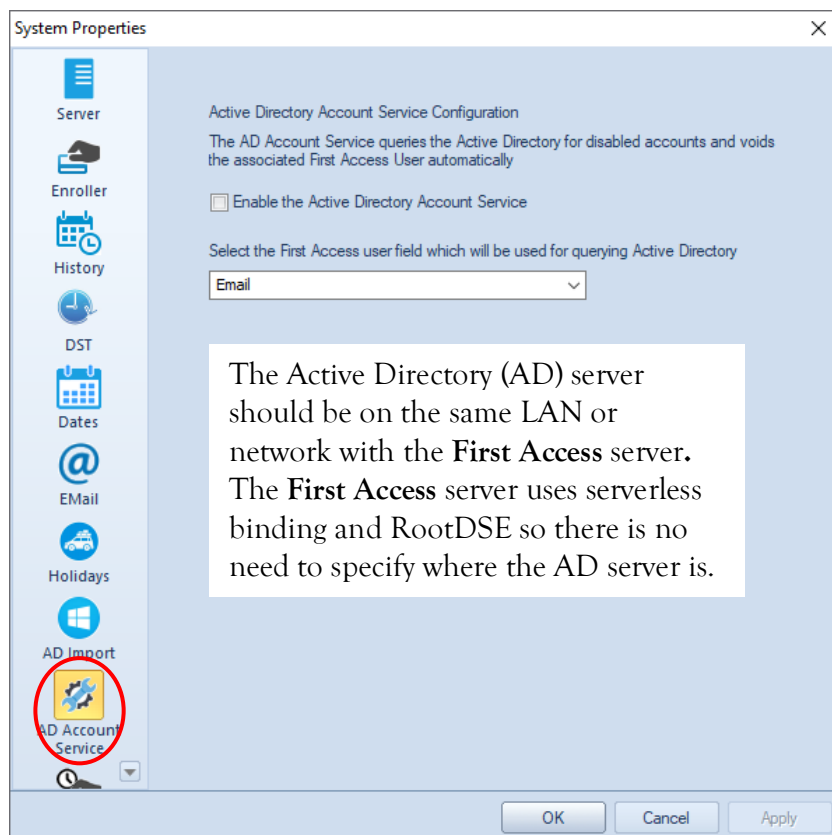
Sample user attributes



User Fields can be defined from here

ACTIVE DIRECTORY ACCOUNT SERVICE

Active Directory (AD) Account Service is available in First Access Advanced only. This service queries AD for disabled accounts and void corresponding accounts in First Access system.



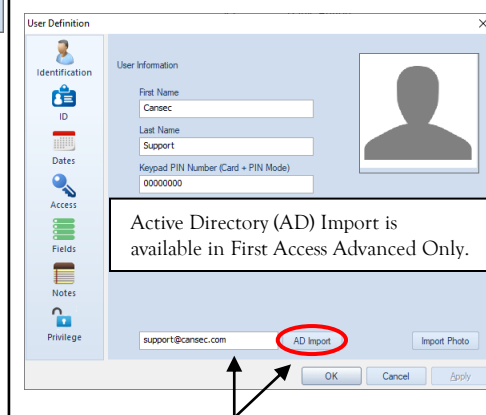
Active Directory attribute for AD queries must be entered for AD Import button and input field to appear or otherwise hidden

Enter the Active Directory attribute for AD queries

mail

Notes:

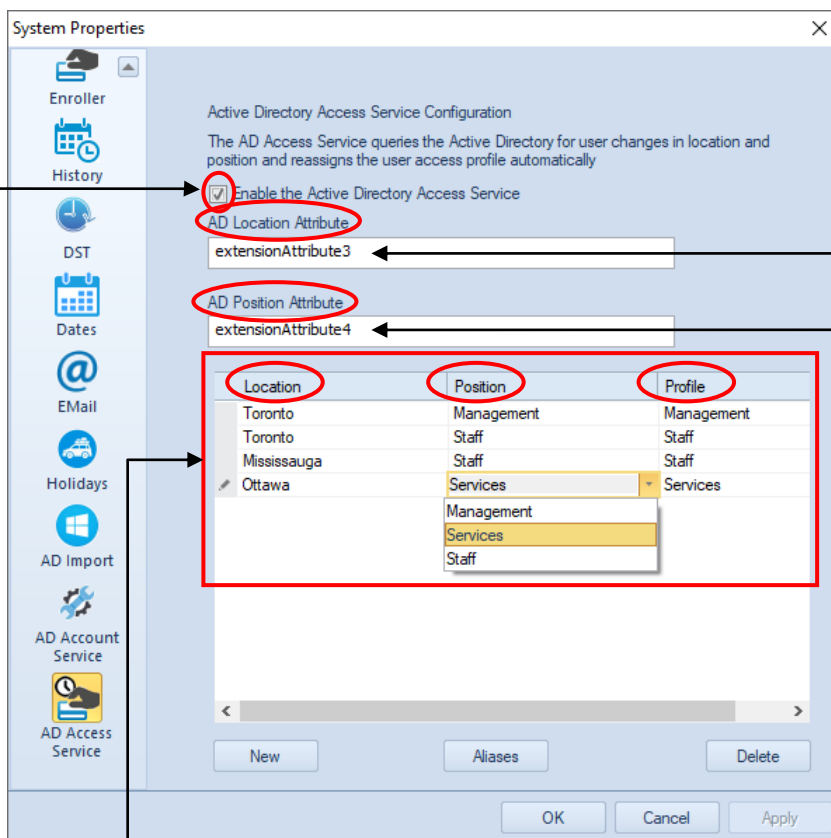
- **First Access** software queries the AD server once every hour for disabled accounts or users and automatically disables those users from the **First Access** database and from the control panels accordingly. If those users are re-enabled from the AD they are not automatically enabled from the **First Access** database or from the control panels.
- Only one way communication from the **First Access** software to the AD server. It does not modify anything in the AD server but only monitors for disabled accounts.
- **First Access** does not automatically update the user fields associated with those attributes if there are changes to those attributes. Use the AD Import button in the user definition page to manually import the changes of the attributes.



ACTIVE DIRECTORY ACCESS SERVICE

Active Directory (AD) Access Service is available in **First Access Advanced** only. The **First Access AD service** has been enhanced to support re-programming of card access based on AD attributes specifying location and job position. The **AD Access Service** queries the Active Directory for user changes in location and position then reassign the user access profile in **First Access** automatically.

Enable this feature by checking the “Enable the Active Directory Access Service” checkbox and enter the two AD attributes which specify the location and job position in the AD schema. The location value will specify one or more location codes or names as defined by the HR or the IT department. All attributes must first be set up by IT personnel.



Location	Position	Profile
Toronto	Management	Management
Toronto	Staff	Staff
Mississauga	Staff	Staff
Ottawa	Services	Services

Sample attributes only. Your IT personnel may use a different attribute

1. This table maps location and position values to a defined access profile. While location values specify strings as they would appear in AD, the job position entry specifies predefined aliases which serve as placeholders for a group of one or more job position strings. The job position aliases are selected from the column entries drop list. Finally the access profile associated with the two previous location and job code values is selected from its column entry drop list.

- To create a new location select **New** and enter location name. Assign desired position and access profile to this location. If there are multiple positions at a location then repeat the same step to create a new location sharing the same location name then assign it with a different position and a corresponding access profile.

Location	Position	Profile
Toronto	Management	Management
Toronto	Staff	Staff
Mississauga	Staff	Staff
Ottawa	Services	Services
New Aliases Delete		

- To delete a location select a location and select **Delete**

Location	Position	Profile
Toronto	Management	Management
Toronto	Staff	Staff
Mississauga	Staff	Staff
Ottawa	Services	Services
New Aliases Delete		

- To add/modify/delete aliases select **Aliases**. Select **New** to create a new alias and enter associated job codes. If necessary select an existing alias and select **Delete** to delete it.

The alias name maps multiple HR job position codes to a single alias name. The job code value will specify one of the predefined job codes created by HR or IT

Ensure that an alias to be deleted is not actively in use in the mapping table. This will cause the table column entry to be blank and the table will not be saved

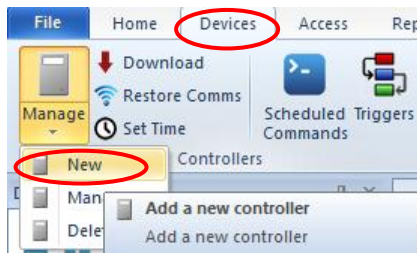
AD Access service periodically scans the defined First Access user database and queries the AD user object by using the user defined field e.g. Email in the AD Account Service tab. If successful, the values associated with the location and position attributes are retrieved and a look up is performed. If a match is made the access profile of the user is compared against the access profile defined in the table. If they do not match, the First Access user is assigned the new access profile and system updates the card access at associated card readers.

Step 3. Panel and Reader Definition

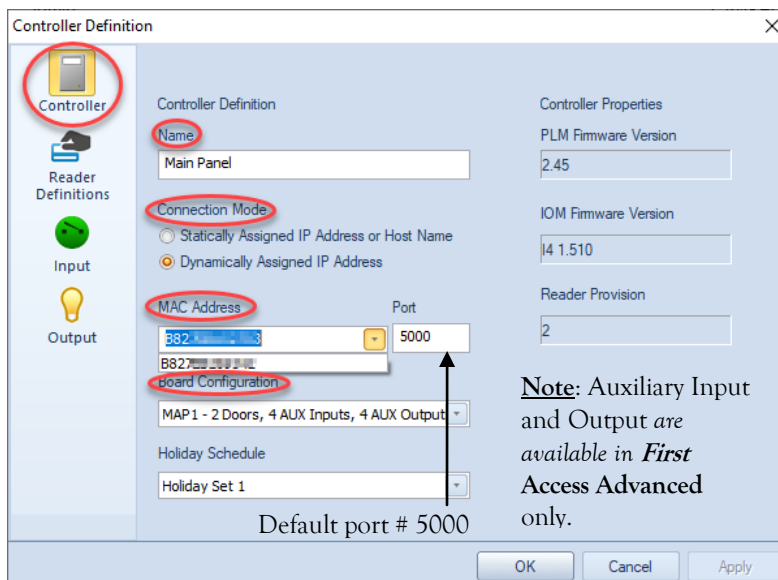
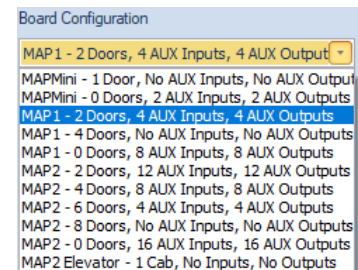
ADD PANEL

1. Select **Devices>Manage>New**.

Note: *Scheduled Commands and Triggers are available in First Access Advanced only.*

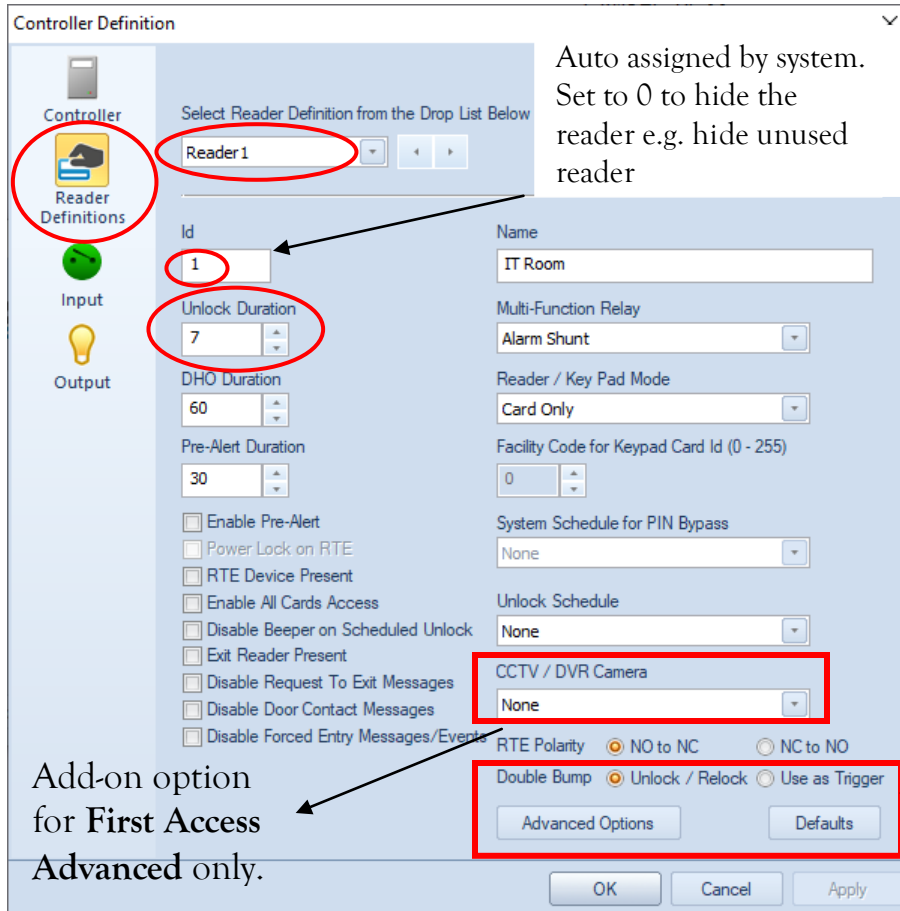


2. Enter a name for the panel, e.g. *First Panel*. By default, all MAP panels are set to obtain an IP address automatically. Select **Dynamically Assigned IP Address** and select the MAC address associated with the panel. If you set a static IP address for the panel (see *Installation Guide for IP Address and Port configuration*) then select **Statically Assigned IP Address or Host Name**, and enter the IP Address or the host name and the port number of the panel. Select board configuration. The factory default configuration is 2 Doors. *Optionally it can be upgraded via purchasing a provisioning file.* Controller properties will be shown when communication is established.



ADD READER

1. Select **Reader Definitions**. Reader Id is auto-generated by selecting it. **Note:** Reader with Id 0 is an undefined reader. Each reader has its own unique Id. Use the drop-down arrow or the left and right arrows to get to the desired reader.



Controller Definition

Auto assigned by system. Set to 0 to hide the reader e.g. hide unused reader

Select Reader Definition from the Drop List Below

Reader1

Id: 1

Unlock Duration: 7

DHO Duration: 60

Pre-Alert Duration: 30

Enable Pre-Alert

Power Lock on RTE

RTE Device Present

Enable All Cards Access

Disable Beeper on Scheduled Unlock

Exit Reader Present

Disable Request To Exit Messages

Disable Door Contact Messages

Disable Forced Entry Messages/Events

Name: IT Room

Multi-Function Relay: Alarm Shunt

Reader / Key Pad Mode: Card Only

Facility Code for Keypad Card Id (0 - 255): 0

System Schedule for PIN Bypass: None

Unlock Schedule: None

CCTV / DVR Camera: None

RTE Polarity: NO to NC, NC to NO

Double Bump: Unlock / Relock, Use as Trigger

Advanced Options

Defaults

OK

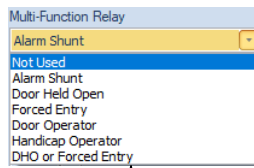
Cancel

Apply

Note:
Auxiliary Input and Output are available in **First Access Advanced** only.

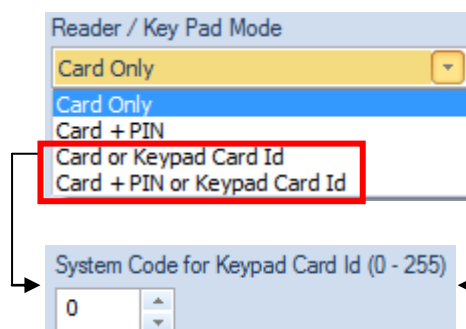
Note:
Available in **First Access Advanced** only.

2. Select an unlock duration, in seconds (60 seconds max.), for the door when a valid credential is presented or when an exit button is pressed.
3. Select a **DHO** (Door Held Open) time (300 seconds max.) for the panel to wait before activating the multi-function relay when the door is left open for too long. This requires the door to have a door contact installed and the multi-function relay configured as **Door Held Open** relay.
4. Select a pre-alert time for the reader to emit a warning tone when the door is left open for too long before it initiates a constant reader beep. The pre-alert time is greater than the unlock time but less than the DHO time.
Note: In the example image above, the Pre-Alert Duration is set to 30 seconds.
5. Enter a name for the reader, e.g. *Front Door* or *IT Room*.
6. Select the desired function to assign to the multi-function relay. This relay can be assigned to only one of the following functions:



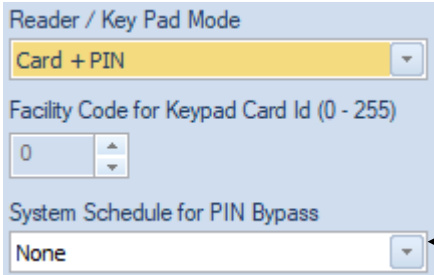
Not Used	<i>This relay is not used at all.</i>
Alarm Shunt	<i>This relay is used to shunt an alarm when an access granted or an exit button event occurs. When used, this relay is activated prior to the lock relay's activation and deactivated after the door contact is closed. If door contact is not used then it's deactivated when the lock is relocked.</i>
Door Held Open	<i>This relay is used to activate another device (e.g. an external light strobe or alarm) when the door is held open longer than the pre-set time.</i>
Forced Entry	<i>This relay is used to activate another device (e.g. an external light strobe or alarm) when the door is forced open without a valid credential or an exit button press.</i>
Door Operator	<i>This relay is used to activate a door operator after an access-granted or an exit button event occurs.</i>
Handicap Operator	<i>This relay is used to activate a door operator only when a valid credential, <u>designated as handicap credential</u>, is presented at a reader. Exit button event also activates this relay.</i>
DHO or Forced Entry	<i>This relay is used to activate another device (e.g. an external light strobe or alarm) when the door is held open longer than the pre-set time or when the door is forced open without a valid credential or an exit button press.</i>

7. Select an optional unlock schedule. There are 255 available unlock schedules. The unlock schedule, when defined and used, allows the door to automatically unlock and relock at pre-defined times. If not used, select **None**.
8. If using keypad select one of the available modes below.



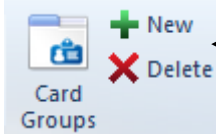
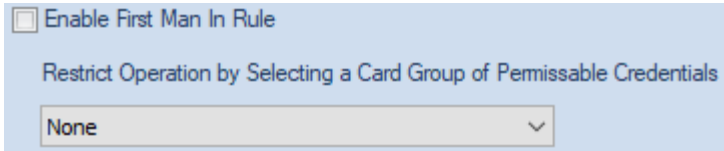
4-bit-burst keypad required. Preferably Cansec tested keypads.

System/Facility Code (between 0 and 255 inclusive) must be entered whenever *Keypad Card Id* is involved. Not required for **Card Only** mode or **Card + PIN** mode.

Card Only	Only cards or card numbers entered as a PIN.
Card + PIN  4-bit bust programming card provided with Cansec P-620 or P-640 keypad	Card presentation followed by PIN entered from keypad. Optionally, select a system schedule you have defined to bypass PIN requirement. 
Card or Keypad Card Id (For P-620 or P-640 keypad, use provided 4-bit bust programming card to program the keypad. See keypad manual for more info)	Card presentation or use keypad to enter card number e.g. (asterisk) * card number # (pound)
Card + PIN or Keypad Card Id (For P-620 or P-640 keypad, use provided 4-bit bust programming card to program the keypad. See keypad manual for more info)	Card presentation followed by PIN entered from keypad or use keypad to enter card number e.g. (asterisk) * card number # (pound)

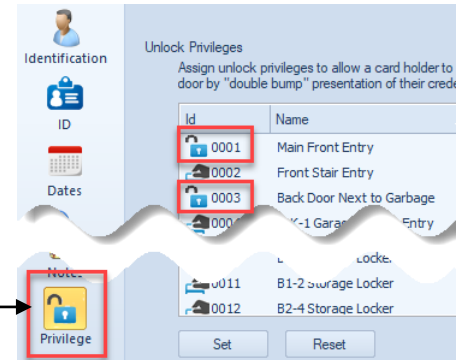
9. Select optional features below.

Enable Pre-Alert	Enable reader warning tone when the door is held open longer than preset time.
Power Lock on RTE	Activate the lock and shunt the door contact when RTE (Request To Exit) button is pressed. If unselected, only the door contact is shunted. This option allows the installer to install an indoor motion sensor hooked up to RTE to trigger a valid egress without generating a forced entry when the door is opened from inside.
Enable First-Man-In Rule	If this rule is enabled, the door will <u>not</u> automatically unlock (based on its selected unlock schedule) until the first valid credential is presented at the reader. If no unlock schedule is used then this option has no effect. <u>First Access Express:</u> When selected, the rule applies to all valid credentials ☐ Enable First Man In Rule

	<u>First Access Advanced:</u> Select  to show “Enable First Man In Rule” option. When selected, you have options to select a predefined group of credentials the rule should apply to or select none for the rule to apply to all valid credentials.  Use this option to create Card Group(s) 
Enable All Cards Access	Granting access to all cards (up to 64-bit) with or without being registered in the system. This option should be used with discretion and must be disabled when all cards have been registered in the system.
Disable Beeper on Scheduled Unlock	The beeper of the reader normally beeps when the door is unlocked on a schedule. However, the beeper can be disabled by selecting this option.
Exit Reader Present	Indicates that there is an exit reader mounted on the egress side of the door. This reader is wired up to the same port of the entry reader mounted on the ingress side of the door. See installation guide.
Disable Request To Exit Messages	Disable request to exit messages from being displayed and recorded in the software.
Disable Door Contact Messages	Disable door contact messages from being displayed and recorded in the software.
Disable Forced Entry Messages/Events	Disable forced entry messages from being displayed and recorded in the software. Also disable the forced entry event. Door open/close messages are shown instead.
RTE Device Present	Check off if Request-To-Exit device is installed. If no RET device is installed then the controller will not monitor forced entry event but door open/close and door-held-open events only.
Default Button	Reset all options above to default.

10. RTE (Request To Exit) Polarity can be set to either Normally Open (NO to NC) or Normally Close (NC to NO) depending on the configuration of the RTE device.
11. Double Bump/Tap (Double Card Swipe) can be used to unlock/relock a door or it can be used as a trigger.

- Unlock/Relock: Performs just one function which is toggling the lock.
- Used as Trigger: Performs one of the functions other than just unlock/relock. See *Trigger section for more information.*



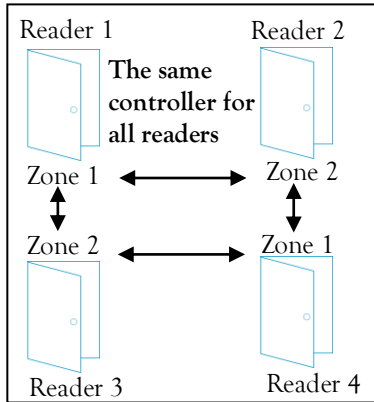
12. Advanced options are available in **First Access Advanced** only.

Used as Trigger requires Unlock Privileges to be set for certain cardholders that need it e.g. Management Staff.

13. Select one of the options below for each individual reader.

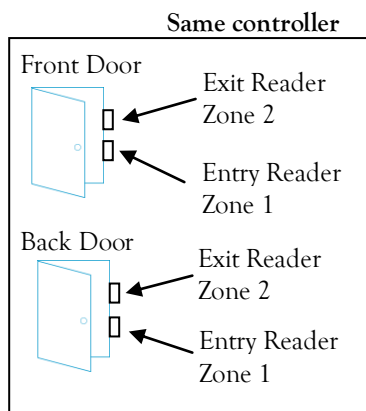
Disable APB	<i>APB is not enforced on this reader.</i>
Enable Timed APB	<i>Once a credential is used at this reader, it can be re-used at this reader only after the APB time, in minutes (2 to 60), has elapsed.</i>

Enable Zone Based APB



In this example, credential accessed any zone 1 reader may access any zone 2 reader. Similarly, credential accessed at any zone 2 reader may access any zone 1 reader.

If a door has an entry reader and an exit reader, the exit reader will be automatically assigned a zone ID one higher than the entry reader e.g. if the entry reader is assigned zone 1 then exit reader will be assigned zone 2 etc... Example below shows that credential entered at either entry reader of front or back door will be able to exit at any exit reader of front or back door.



In this example, credential accessed any zone 1 reader may access any zone 2 reader. Similarly, credential accessed at any zone 2 reader may access any zone 1 reader.

Important: Only readers on the same controller can be grouped into Zones where each member reader has the same zone ID. Grouping readers from different controllers is not supported.

When zone based APB is enabled on a reader, any valid credential, when presented at that reader will be recorded as being in the “to zone”. See example below.

Reader 1: Zone 1 to 2

Enable Zone Based APB

Enter Reader's Member Zone (1 to 8) Enter Reader's To Zone (1 to 8)

Valid credentials presented at reader 1 will be assigned to zone 2, and those credentials can only be used at any member reader of zone 2 or reader that has APB disabled.

Reader 2: Zone 2 to 1

Enable Zone Based APB

Enter Reader's Member Zone (1 to 8) Enter Reader's To Zone (1 to 8)

Valid credentials presented at reader 2 will be assigned to zone 1 and those credentials can only be used at any member reader of zone 1 or reader that has APB disabled.

Reader 3: Zone 2 to 1

Enable Zone Based APB

Enter Reader's Member Zone (1 to 8) Enter Reader's To Zone (1 to 8)

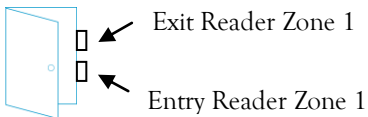
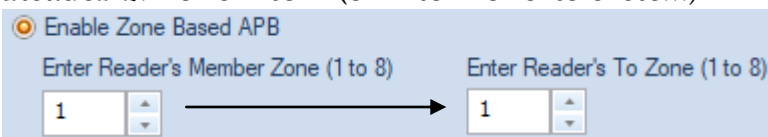
Reader 2 and reader 3 have the same member zone ID. Valid credentials presented at reader 2 or reader 3 will be assigned to zone 1, and those credentials can only be used at any member reader of zone 1 or reader that has APB disabled.

Reader 4: Zone 1 to 2

Enable Zone Based APB

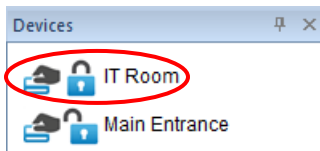
Enter Reader's Member Zone (1 to 8) Enter Reader's To Zone (1 to 8)

Reader 1 and reader 4 have the same member zone ID. Valid credentials presented at reader 1 or reader 4 will be

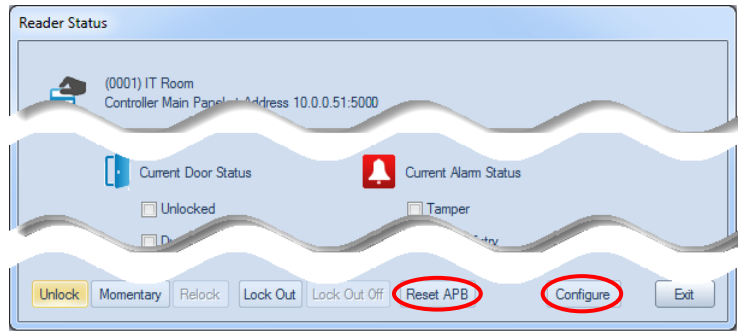
If there is only one door having entry and exit readers participating in zone anti-passback then the member and the enter zone must all be set to the same ID. ID cannot be re-used for other zones. 	assigned to zone 2, and those credentials can only be used at any member reader of zone 2 or reader that has APB disabled Reader 1: Zone 1 to 1 (or 2 to 2 or 3 to 3 etc...)  Just one reader X (X=1, 2, 3 or 4) has entry and exit readers participating in Zone anti-passback. Valid credentials presented at the entry reader will be assigned to exit reader's zone, and those credentials can only be used only at that exit reader or reader that has APB disabled.
Enable Soft APB Mode	Applicable to Zone Based APB only. When soft APB mode is enabled, the controller will grant access to that reader for any valid credential, even if it fails zone verification. However, an event will be recorded indicating that the credential has failed anti-passback verification.
Disable Door Interlock	Door interlock is not enforced on this reader.
Enable Door Interlock	Enforce door interlock on this reader. When enabled, readers that have the same value (1 to 8) assigned will participate in door interlock. Example, if reader A and reader B have value 1 assigned to them then when reader A's door is open, or when reader A's lock is energized then reader B will not grant access to any credential until reader A's lock is de-energized <u>and</u> reader A's door is closed. The same logic applies to reader B. Optionally more than 2 readers can participate in the same or different door interlock zones e.g. readers A, B, C have value 1 assigned or A, B have value 1 assigned and C, D have value 2 assigned etc..

14. When advanced options have been selected and configured then Click **OK** to save settings or click **Cancel** to ignore all settings.

15. To reset Timed or Zone Based APB for all users at a certain reader, double click the desired reader displayed in the device panel.

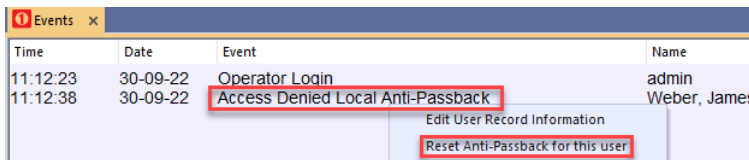


16. Click **Reset APB**. This will clear APB for all users at this reader.



17. To reconfigure the reader, click **Configure**. Click **Exit** when done.

Note: To reset Timed or Zone Based APB for an individual user who got access denied due to APB at a reader, right click on the event or the user name in the Event View and reset Anti-Passback for that user.

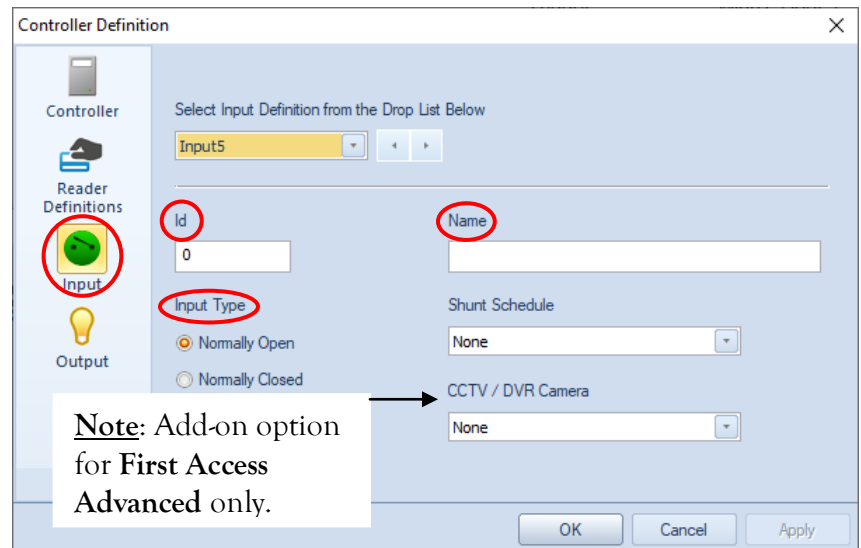


DEFINE AUXILIARY INPUT POINT

Note: Auxiliary Input and Output are available in **First Access Advanced** only.

If the panel is provisioned with 2 doors then there are 4 auxiliary inputs available for use. If the panel is provisioned with 4 doors then there are no auxiliary inputs available for use.

1. Select **Input** icon from the left panel.
2. From the right panel, select an available input point from the drop list.
3. Use system-assigned ID or manually enter an un-assigned ID e.g. 1, 2 or 3 etc... for this input point. Each input point has a unique ID.



4. Enter an appropriate name for the input point e.g. Panic Button.
5. Select a type for the input point e.g. **Normally Open** or **Normally Closed**.

- Optionally, select a defined shunt schedule to shunt the input event from being processed. A shunt schedule must be manually defined. A shunt schedule can be used to ignore or to process input events at different times. Otherwise select **None** for events to be processed at all times.

DEFINE AUXILIARY OUTPUT POINT

Similar to input point configuration, if the panel is provisioned with 2 doors then there are 4 auxiliary outputs available for use. If the panel is provisioned with 4 doors then there are no auxiliary outputs available for use.

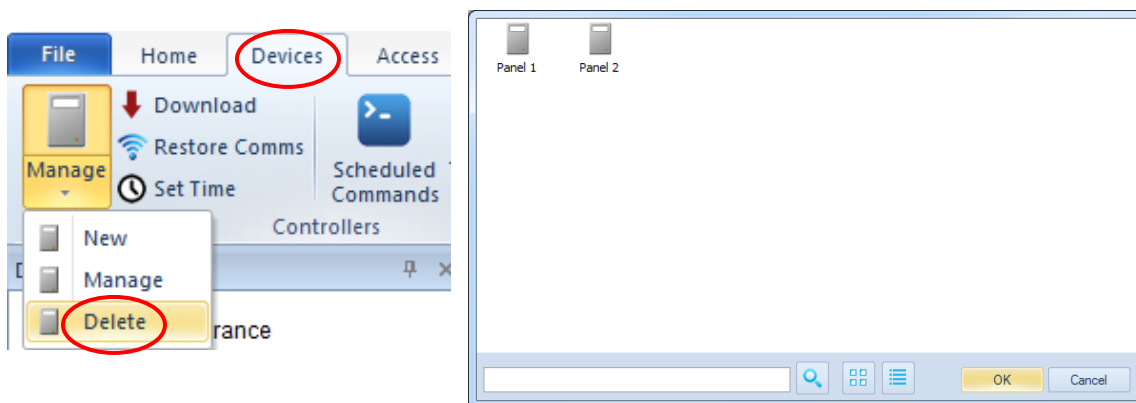
- Select **Output** icon from the left panel.

Note:
Auxiliary
Input and
Output are
available in
**First Access
Advanced**
only.

- From the right panel, select an available output point from the drop list.
- Use system-assigned ID or manually enter an un-assigned ID e.g. 1, 2 or 3 etc... for this output point. Each output point has a unique ID.
- Enter an appropriate name for the output point e.g. Alarm Horn.
- Optionally select a defined output schedule to automatically activate the output point. Output schedules must be defined by the operator before they can be selected. An output can be used to activate or deactivate a device based on a schedule. Otherwise, select **None** if no schedule is assigned.

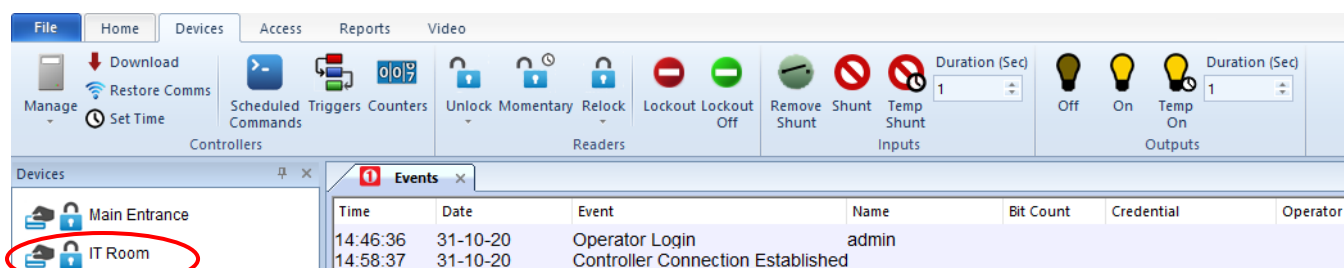
EDIT AND DELETE PANEL

1. To edit a panel select **Devices>Manage**, or select **Devices>Delete** to delete a panel.

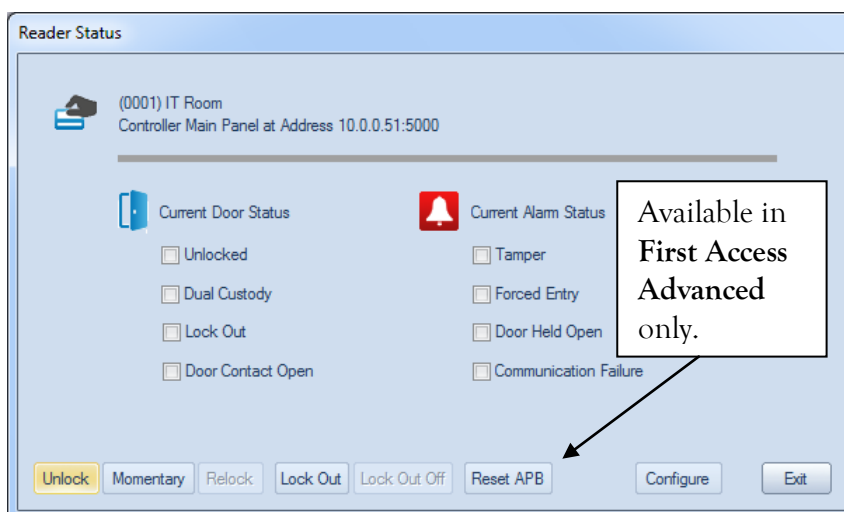


2. Select a panel and click OK.

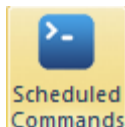
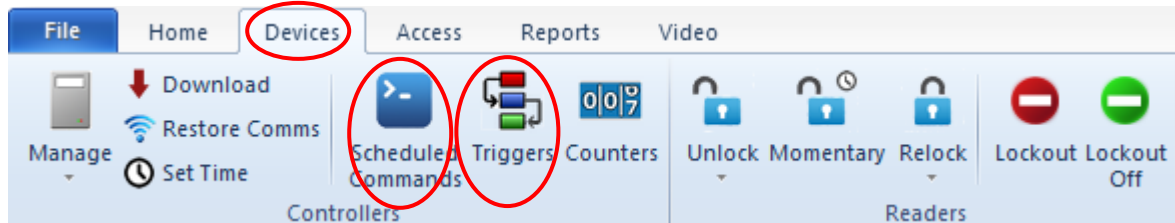
READER STATUS



Click on a reader to view its status. Status notifications will be indicated by a check mark in the appropriate box.



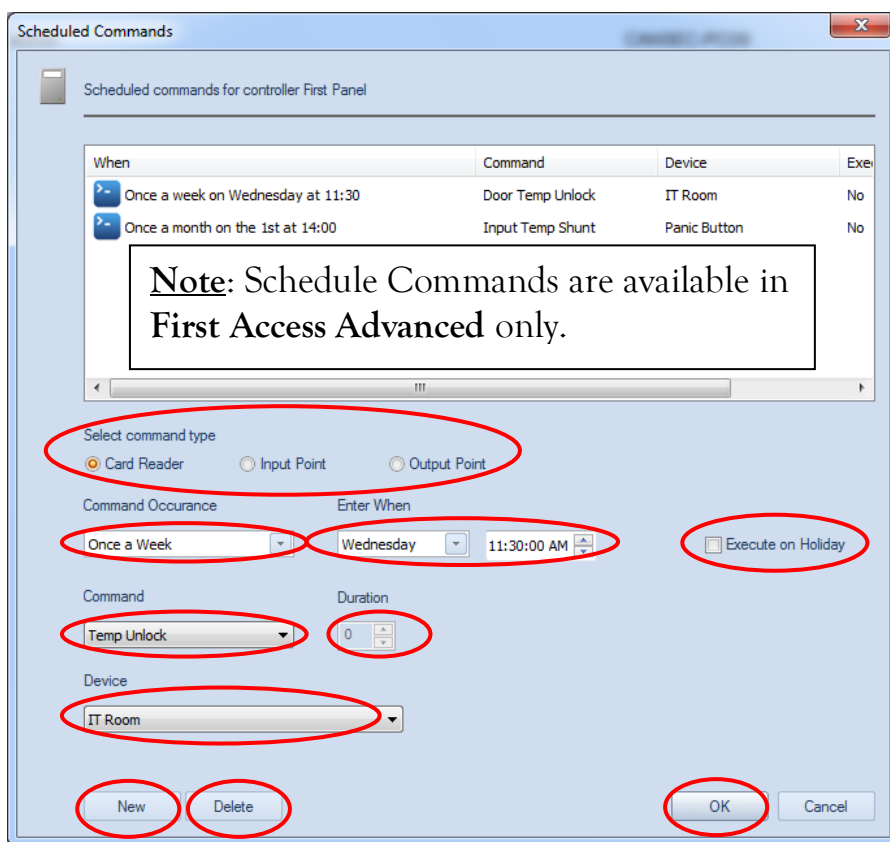
READER COMMANDS, SCHEDULED COMMANDS, TRIGGERS, COUNTERS



➤ Scheduled Commands

Note: Schedule Commands are available in **First Access Advanced** only.

Scheduled commands are used to command locks, input point and output point based on a schedule that is different from the weekly schedule.



Note: Only 200 Schedule Commands are available per panel.

1. Click Scheduled Commands and click **New**
2. Select a desired reader

3. Select a command type

4. Select Command Occurrence.

5. Enter the day and time when the command will occur and select if it should be executed on a holiday.

6. Select the command that should be applied to the device

Commands for Reader

Commands for input

Commands for output

Duration (maximum value is 1000 seconds) is applicable only to Input Temp Shunt and Output On Temp

Unlock	Unlock the lock. The lock remains unlocked.
Temp Unlock	Temporary unlock the lock and relock after the unlock time has expired.
Relock	Relock the lock.
Lockout On	Disable the card reader. Card reader flashes red and green. Only credentials with lockout-bypass exemption will be granted access.
Lockout Off	Enable the card reader and remove it from the lockout state.
Input Shunt	Input events from the input point will not be processed at all.
Input Temp Shunt	Temporarily suspend processing of input events from this input point until the duration has expired.
Remove Shunt	Disable shunt and resume processing input point events normally.
Output On	Activate the output point.
Output On Temp	Temporarily activate the output point for the configured duration.
Output Off	Deactivate the output point.

7. Click OK to save settings.

Command Information:

Select a command to be performed on another device when an event from a certain device occurs. The delay time can be optionally set before the command is executed. The system schedule must be used to schedule the command or otherwise the command will not be executed.

Command Information

Command Delay Duration (Secs) Command Duration Device Schedule

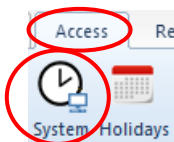
OK Cancel

- Reader Unlock
- Reader Relock
- Reader Momentary
- Output On
- Output Off
- Output Momentary
- Input Shunt
- Input Shunt Remove
- Input Shunt Momentary
- Reader Lockout On
- Reader Lockout Off
- Reader Lock Toggle
- Output Activate Toggle
- Reader Lockout Toggle
- Input Shunt Toggle
- Counter Increment
- Counter Decrement
- Counter Add
- Counter Subtract
- Counter Set

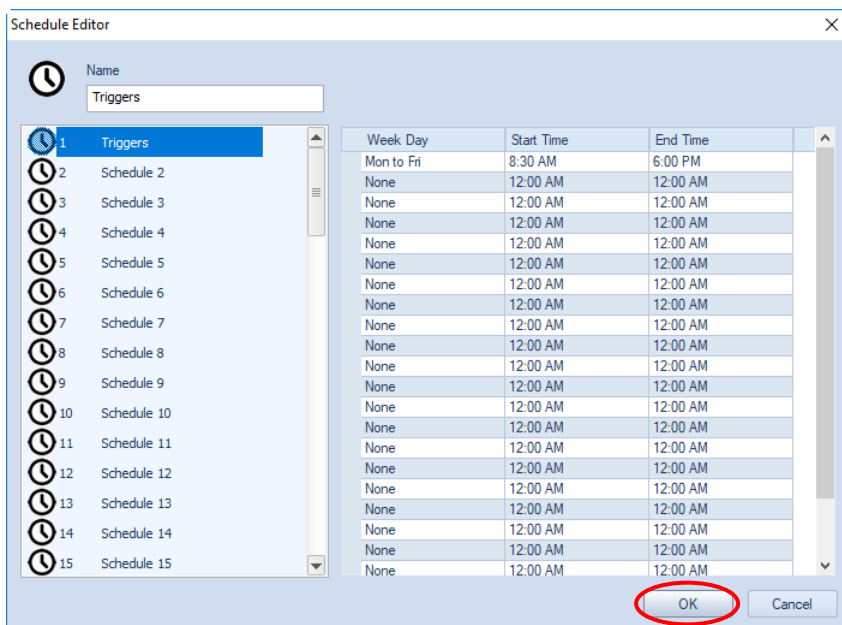
Reader Unlock	Unlock reader
Reader Relock	Relock reader
Reader Momentary	Unlock reader momentarily
Output On	Activate output
Output Off	Deactivate output
Output Momentary	Activate output momentarily
Input Shunt	Shunt or deactivate input
Input Shunt Remove	Remove input from being shunted
Input Shunt Momentary	Momentarily remove input from being shunted
Reader Lockout On	Lock out or lock down reader.
Reader Lockout Off	Remove reader from being locked out
Reader Lock Toggle	Toggle the lock from locked to unlocked or vice versa
Output Activate Toggle	Toggle the output from ON to OFF or vice versa
Reader Lockout Toggle	Toggle the reader lock out from ON to OFF or vice versa
Input Shunt Toggle	Toggle the input from shunted to un-shunted or vice versa
Counter Increment	Increment the counter by 1.
Counter Decrement	Decrement the counter by 1.
Counter Add	Add counter with a number predetermined by the user
Counter Subtract	Subtract counter with a number predetermined by the user
Counter Set	Set counter to a specific value predetermined by the user

In the example below, there is only one panel named **Main Panel**. However, in some situations there could be many panels. We will implement a trigger on this Main Panel such that when the Main Entrance is momentarily unlocked, the panel will delay for 3 seconds then activates an output point connected to a Parking Gate for 10 seconds.

1. From the top menu select **Access** then select **System**

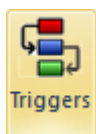
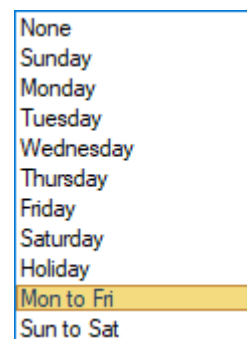


2. Select one of the available schedule and name it *Triggers* or some other name

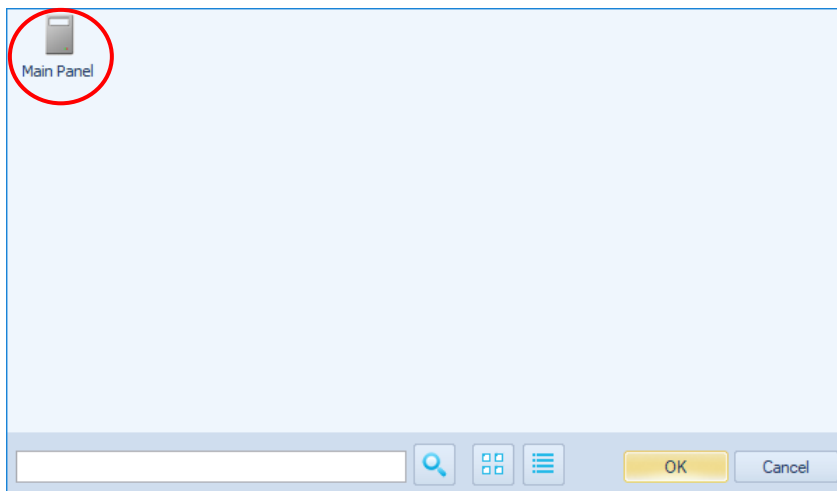


3. Set the execution time from Monday to Friday between 8:30 AM and 6:00 PM

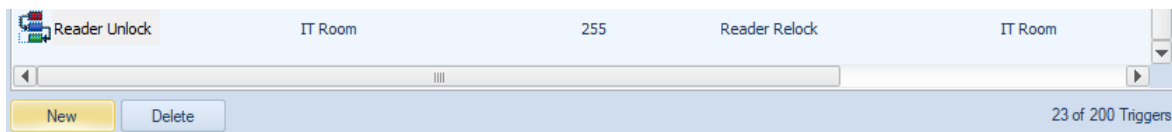
Note: Other options are available for Week Day as seen below



4. Select **Triggers** from the top menu
5. Select **Main Panel** from the list to have triggers implemented on.



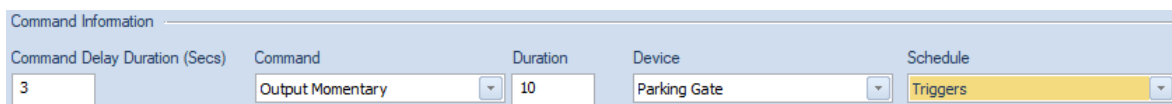
6. Click **New** to add a new trigger.
7. Select or highlight the newly added trigger normally found at the bottom of the list.



8. Select *Reader Momentary* from **Event** drop-down list and select *Main Entrance* from the **Device** drop-down list. Other events may be used e.g. *Double Bump Event*.



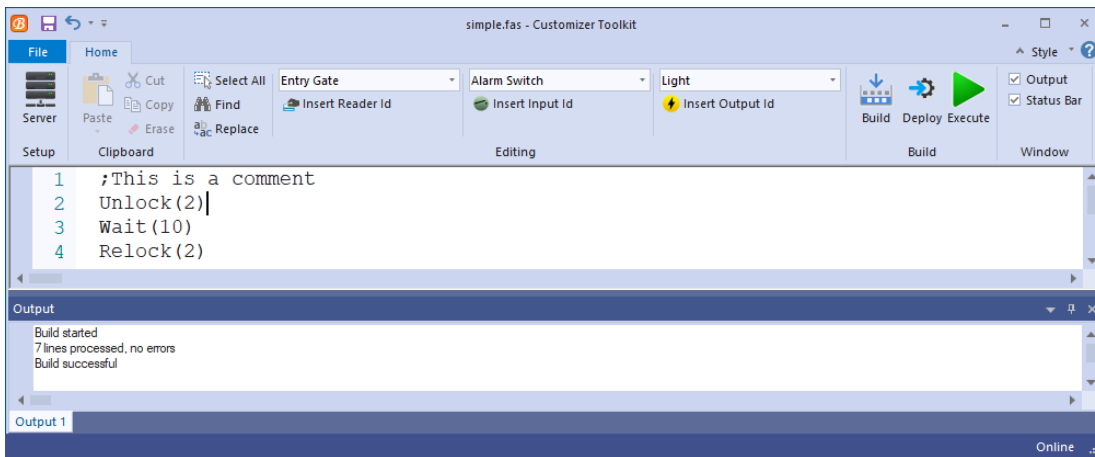
9. Under **Command Delay**, enter 3. Under **Command** select *Output Momentary*. For **Duration** enter 10. Under **Device** select *Parking Gate* and under **Schedule** select *Triggers* which is the schedule we have previously defined.



10. Click **New** to add additional triggers or click **OK** to finish. New added triggers will be downloaded to the panel automatically.

➤ Customizer Module Triggers

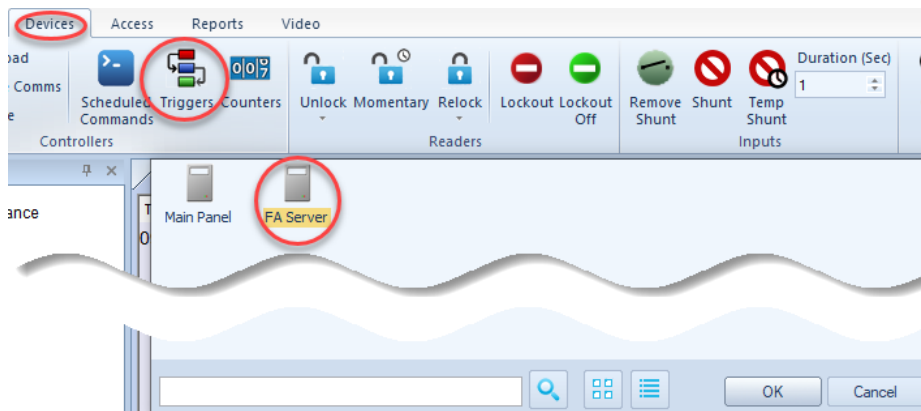
Customizer Module Triggers (*maximum 200 triggers per server*) are similar to controller triggers except that they can be used to respond to events that happen to a single or multiple panels. For example, when access is granted at a particular panel, the customizer module trigger can be used to perform actions not only on that particular panel but also on other remote panels. These actions are achieved by means of customizer modules written using FA Customizer Toolkit. *Download and view FA Customizer Toolkit Guide from Cansec website for more information.*



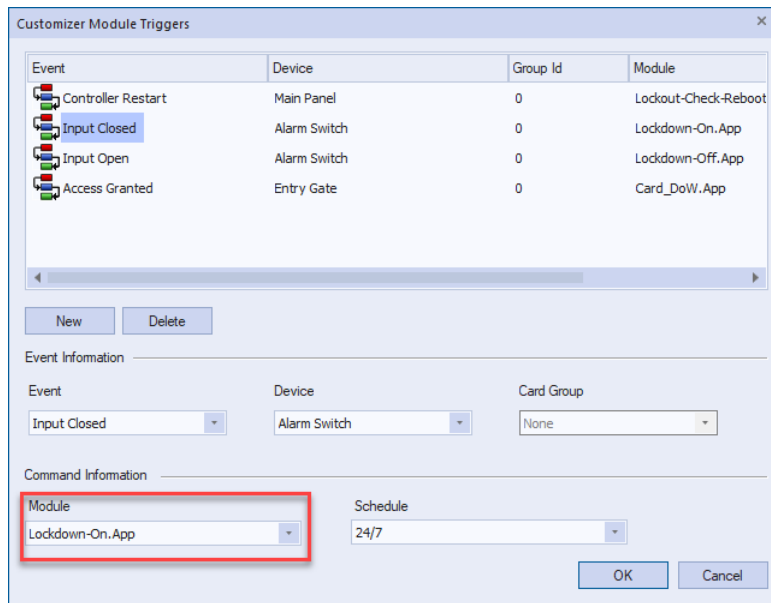
Example: An input point on a certain panel when closed will cause the reader with id #2 to unlock for 10 second then relock.

Note: Each reader has its own unique id and readers can be on the same or different panels. Each panel also has its own unique MAC address and IP address making it easier for the server triggers to indentify and send instructions to the exact panel and exact reader.

1. From Devices menu, select Triggers and select FA Server.

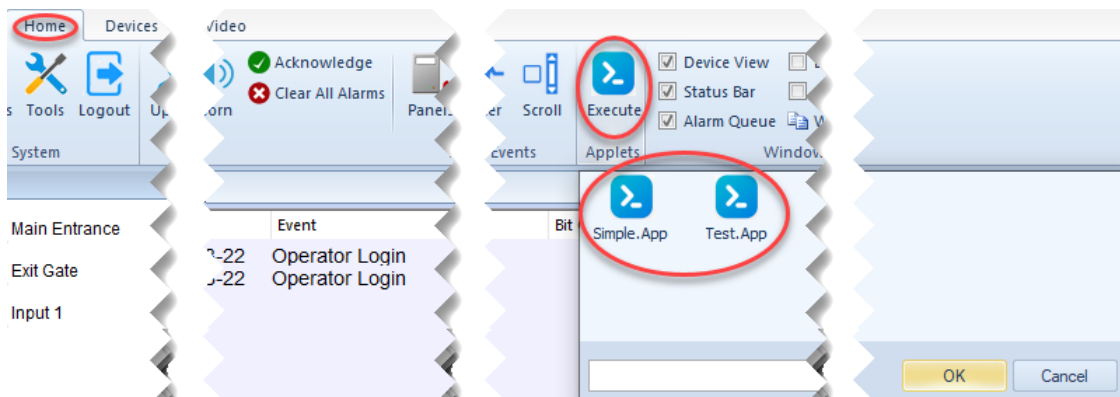


2. Select an event, in this case Input Closed, and select which panel or device the input point is located from. Select which customizer module to run and which schedule to follow



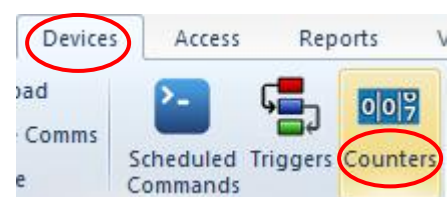
➤ Customizer Module Execution

Each Customizer Module, once created, compiled and deployed, can be manually selected and executed.



➤ Controller Counters

There are 40 counters available per controller. Each counter can be used for different purposes. For example, a counter can be used to count the numbers of cars entering and exiting a parking lot, and when a threshold is met it automatically



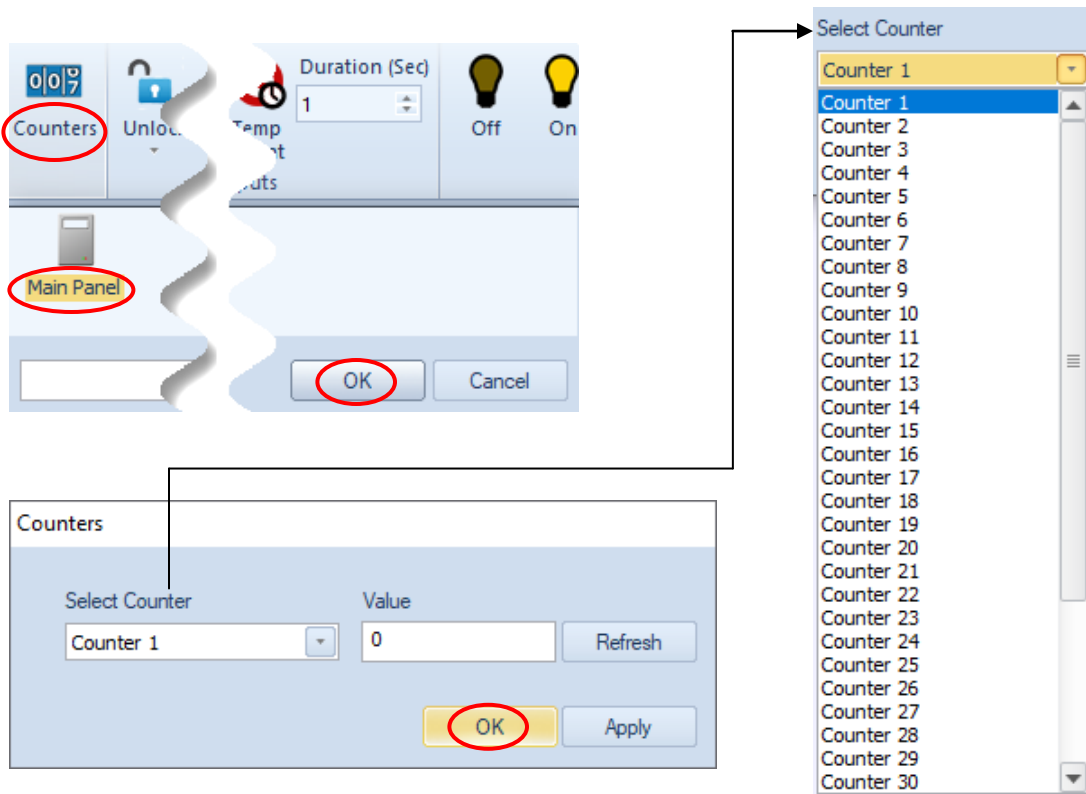
activates an output hooked up to digital signage to display the occupancy status of the parking lot.

Example:

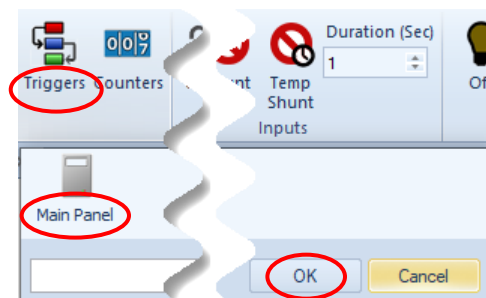
- When a car enters the entry gate, the controller increments the counter by 1. If the counter reaches the threshold, the controller activates an output point hooked up to a digital signage to show the lot is full and at the same time lockouts the entry gate.
- When a car exits the exit gate, the controller decrements the counter by 1. If the counter reaches below the threshold, the controller deactivates the output point to turn off the digital signage and at the same time remove the lockout for the entry gate.

In this example we use Counter 1 but you may use other counters

1. View and set counter 1 of the Main Panel to a desired starting value e.g. 0 etc...



2. Create triggers



3. Select **New** to create a new trigger

The screenshot shows the 'Controller Triggers' dialog box. At the top, there is a table with columns: Event, Device, Group Id, Command, and Device. Below the table, there are 'New' and 'Delete' buttons. The 'New' button is circled in red. To the right of the buttons, it says '0 of 200 Triggers'. Below the buttons, there are two sections: 'Event Information' and 'Command Information'. The 'Event Information' section has fields for Event, Device, Card Group, and Value. The 'Command Information' section has fields for Command Delay Duration (Secs), Command, Duration, Device, and Schedule. At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Select the new added trigger and change the event to **Access Granted** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

The screenshot shows the 'Controller Triggers' dialog box with a trigger configuration. The table at the top has one row: Event: Reader Unlock, Device: Entry Gate, Group Id: 255, Command: Reader Relock, Device: Entry Gate. Below the table, there are 'New' and 'Delete' buttons. A text box with the text 'Increment "counter 1" when a car enters entry gate' has an arrow pointing to the 'Event' field. The 'Event' field is set to 'Access Granted'. The 'Device' field is set to 'Entry Gate'. The 'Card Group' field is set to 'None'. The 'Value' field is set to '0'. The 'Command' field is set to 'Counter Increment'. The 'Duration' field is set to '0'. The 'Device' field is set to 'Counter 1'. The 'Schedule' field is set to '24/7'. The 'OK' button is circled in red. The text '1 of 200 Triggers' is visible on the right.

5. Select **New** again to create a new trigger. Change event to **Access Granted** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

Controller Triggers

Event	Device	Group Id	Command	Device
Access Granted	Entry Gate	0	Counter Increment	Counter 1
Reader Unlock	Entry Gate	255	Reader Relock	Entry Gate

2 of 200 Triggers

New Delete

Decrement "counter 1" when a car exits exit gate

Event Information

Event: Access Granted Device: Exit Gate Card Group: None Value: 0

Command Information

Command Delay Duration (Secs): 0 Command: Counter Decrement Value: 0 Device: Counter 1 Schedule: 24/7

OK Cancel

6. Select **New** again to create a new trigger. Change event to **Counter Equal** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

Controller Triggers

Event	Device	Group Id	Command	Device
Access Granted	Entry Gate	0	Counter Increment	Counter 1
Access Granted	Exit Gate	0	Counter Decrement	Counter 1
Reader Unlock	Entry Gate	255	Reader Relock	Entry Gate

3 of 200 Triggers

New Delete

Activate "Output One" when counter 1 reaches 5

Event Information

Event: Counter Equal Device: Counter 1 Card Group: None Value: 5

Command Information

Command Delay Duration (Secs): 0 Command: Output On Duration: 0 Device: Output One Schedule: 24/7

OK Cancel

In this example, if Output One is hooked up to a digital signage then it will be activated when counter 1 reaches 5.

7. Select **New** again to create a new trigger. Change event to **Counter Equal** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

Controller Triggers

Event	Device	Group Id	Command	Device
Access Granted	Entry Gate	0	Counter Increment	Counter 1
Access Granted	Exit Gate	0	Counter Decrement	Counter 1
Counter Equal	Counter 1	0	Output On	Output One
Reader Unlock	Entry Gate	255	Reader Relock	Entry Gate

4 of 200 Triggers

New Delete

Lockout "Entry Gate" when counter 1 reaches 5

Event Information

Event: Counter Equal Device: Counter 1 Card Group: None Value: 5

Command Information

Command Delay Duration: 7

Reader Lockout On 0 Entry Gate 24/7

OK Cancel

The delay must be set to equal to the unlock time of the gate to allow the car enough time to enter the gate before locking it out

8. Select **New** again to create a new trigger. Change event to **Counter Less Than** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

Controller Triggers

Event	Device	Group Id	Command	Device
Access Granted	Entry Gate	0	Counter Increment	Counter 1
Access Granted	Exit Gate	0	Counter Decrement	Counter 1
Counter Equal	Counter 1	0	Output On	Output One
Counter Equal	Counter 1	0	Reader Lockout On	Entry Gate
Reader Unlock	Entry Gate	255	Reader Relock	Entry Gate

5 of 200 Triggers

New Delete

Remove Lockout "Entry Gate" when counter 1 is less than 5

Event Information

Event: Counter Less Than Device: Counter 1 Card Group: None Value: 5

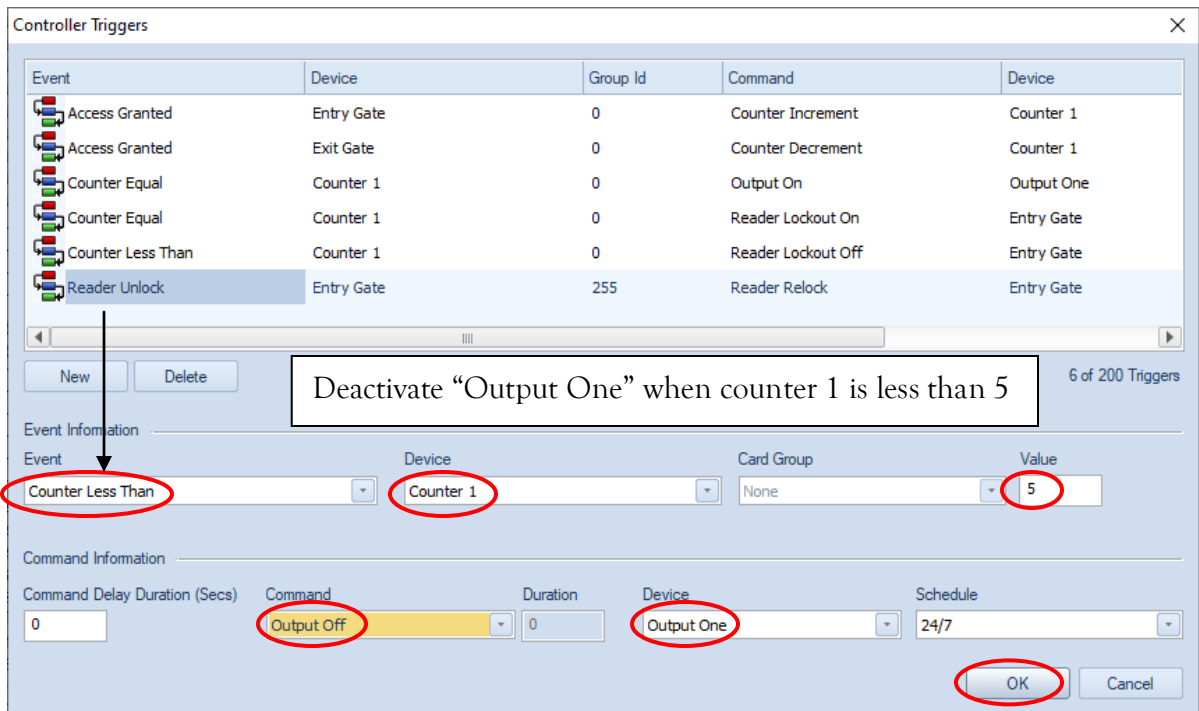
Command Information

Command Delay Duration (Secs): 0

Command: Reader Lockout Off Duration: 0 Device: Entry Gate Schedule: 24/7

OK Cancel

9. Select **New** again to create a new trigger. Change event to **Counter Less Than** and change the appropriate device, command, counter and schedule as seen below. If the selected system schedule is not defined then the trigger will not be executed.

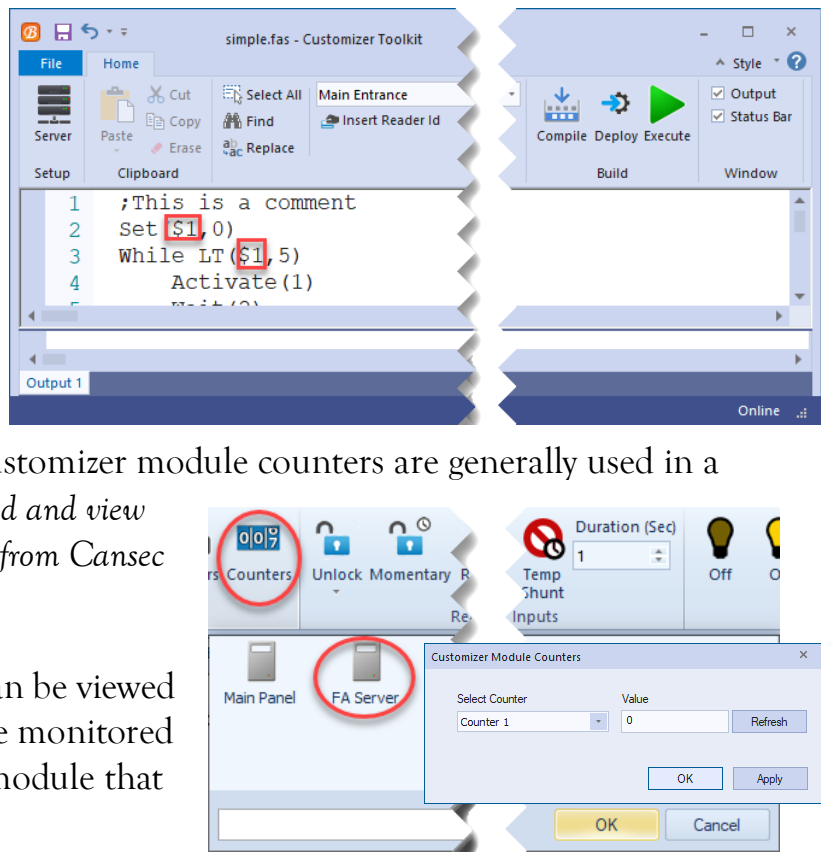


10. Click OK to finish.

➤ Customizer Module Counters

There are 100 customizer module counters available in the First Access server. These counters work the same way as the controller counters do but they reside in the server not in the controllers or panels. The customizer module counters are generally used in a customizer module. *Download and view FA Customizer Toolkit Guide from Cansec website for more information.*

The value of each counter can be viewed or set accordingly and can be monitored when used by a customizer module that has been run.



➤ **Download**

Changes are automatically downloaded and saved to online panels. However, changes made while a panel is offline must be manually downloaded to have them applied.



1. Click Download
2. Select panel(s) and click OK

➤ **Restore Comms**

Restore Comms Provide an immediate attempt to restore communication to offline panels without waiting for an automatic communication-restore process to take effect.

➤ **Set Time**

Manually set the time on all controllers based on host computer's clock. Set time must be done whenever a new panel is added to the system for the panel to have the current date and time. However, the **First Access** software automatically synchronizes the time on all controllers on a daily basis.

Events							
Time	Date	Event	Name	Bit Count	Credential	Operator	Location
11:12:08	08-04-19	System Clock Time Set				admin	Main Panel

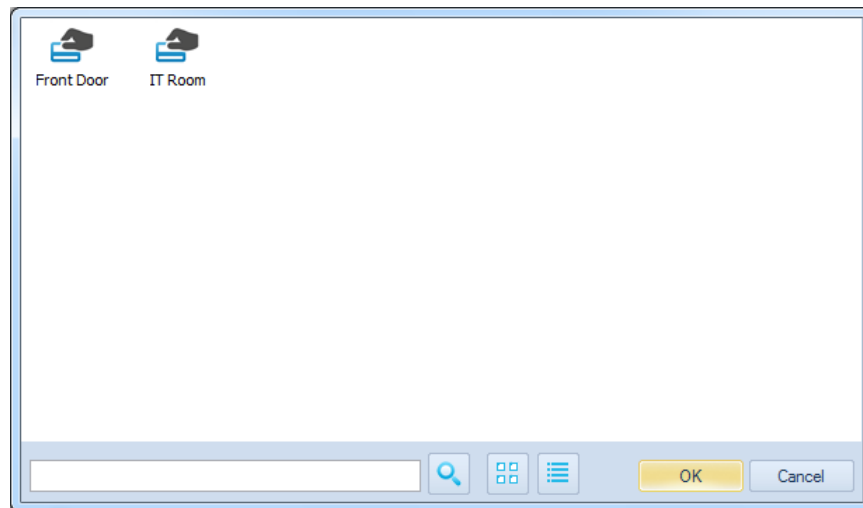
➤ **Unlock, Momentary, Relock, Lockout and Lockout Off**

1. Select an appropriate button, e.g. Unlock, Relock, etc, to perform on the readers.



Unlock	Unlock the lock and keep it unlocked
Momentary	Momentary unlock the lock for the duration set in the unlock time setting of the door
Relock	Relock the lock
Lockout	Relock the lock and disable the card reader from granting access to any credential. Card reader's LED flashes red and green.
Lockout Off	Turn Lockout mode off. Card reader's LED stays solid red and lock remains locked.

2. Select a reader or readers and click **OK**.



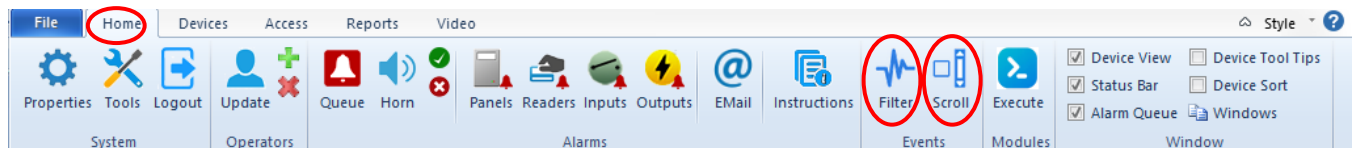
READER EVENTS

All events are recorded in the database and displayed in the Events window.

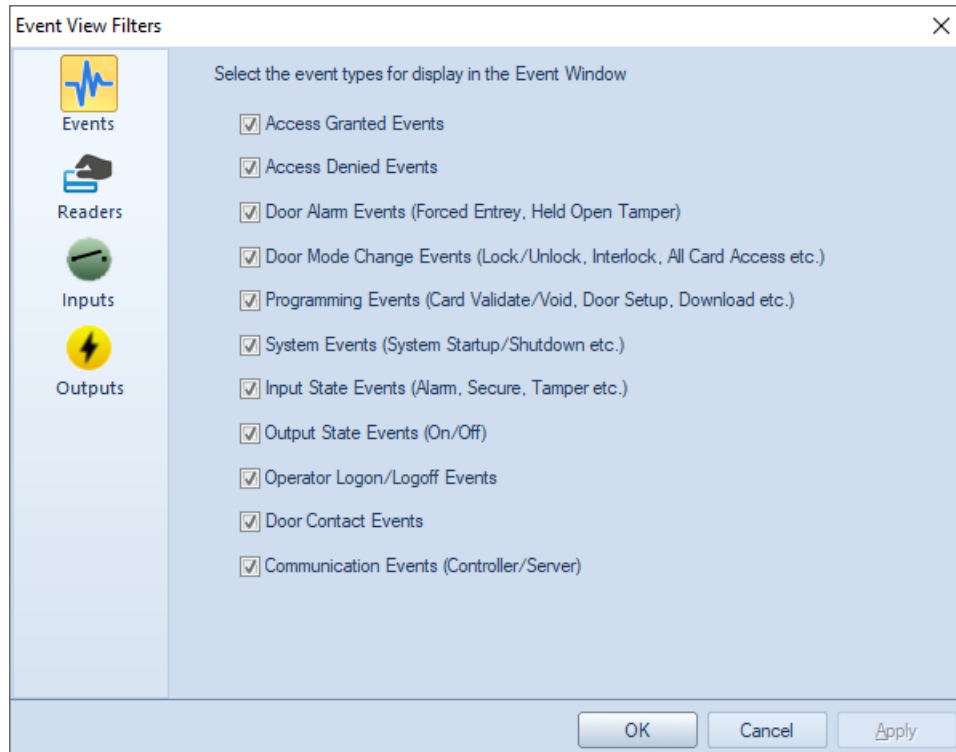
Time	Date	Event	Name	Bit Count	Credential	Operator	Location
16:35:28	03-04-19	Access Granted, Schedule 2	Support, Cansec	37	1603:08471	Reader	IT Room
16:35:33	03-04-19	Request to Exit Pressed				Reader	IT Room
16:35:33	03-04-19	Request to Exit Released				Reader	IT Room
16:35:36	03-04-19	Input Alarm				IO	Panic Button
16:35:36	03-04-19	Input Secure				IO	Panic Button

Events can also be selectively filtered per reader, input/output point and vertical scroll bar can also be enabled in the Event screen.

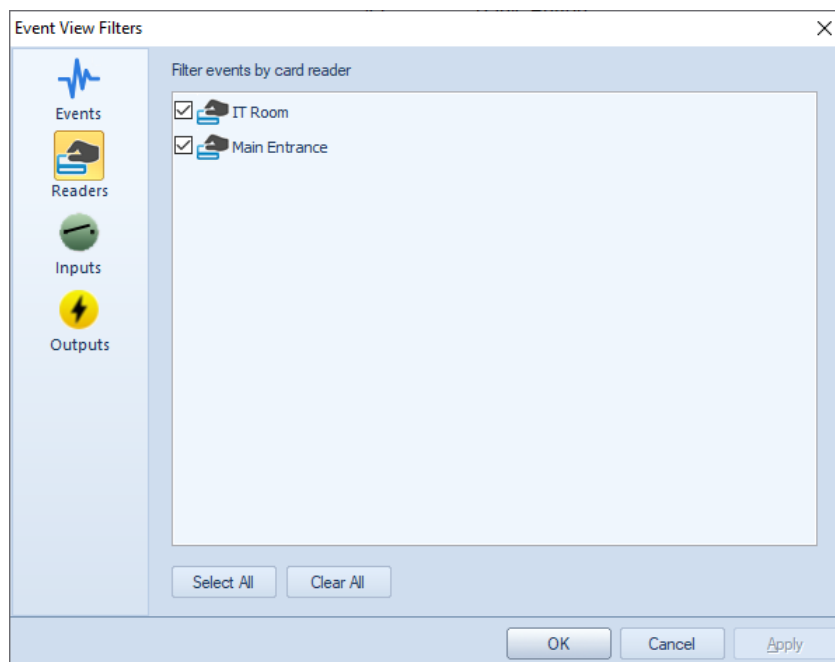
Note: Auxiliary Inputs and Outputs are available in **First Access Advanced** only.



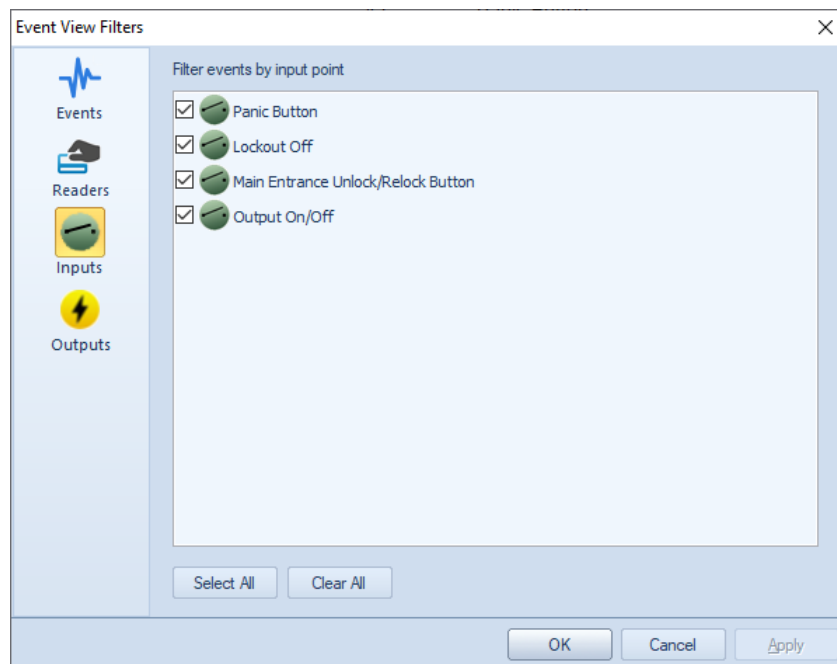
- Event Filter: Select the event types for display in the Event Window



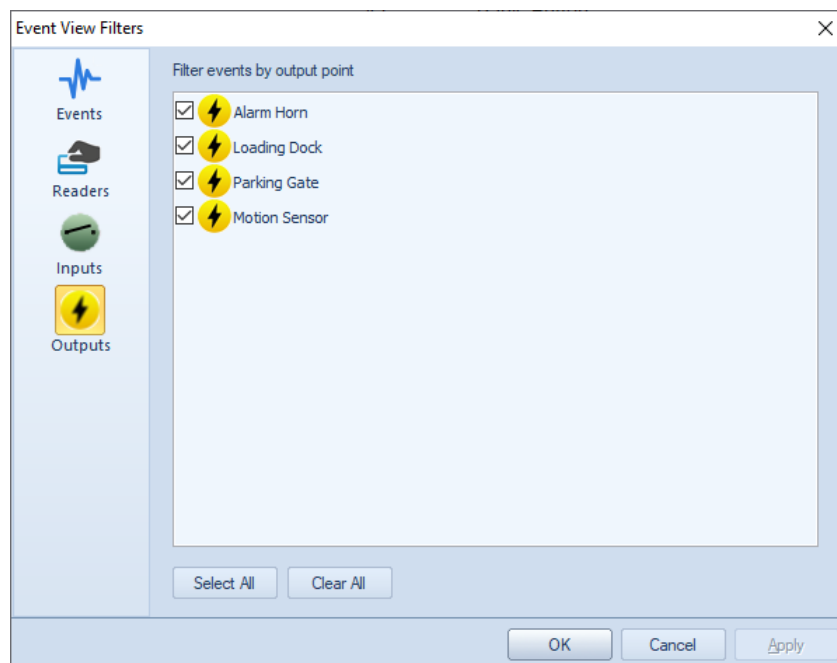
- Reader Filter: Filter events by card reader



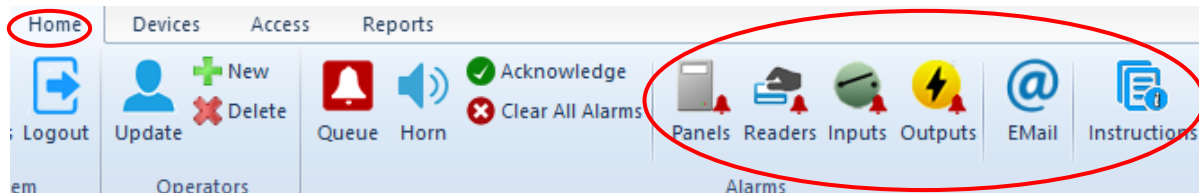
➤ Input Filter: Filter events by input point



➤ Output Filter: Filter events by output point

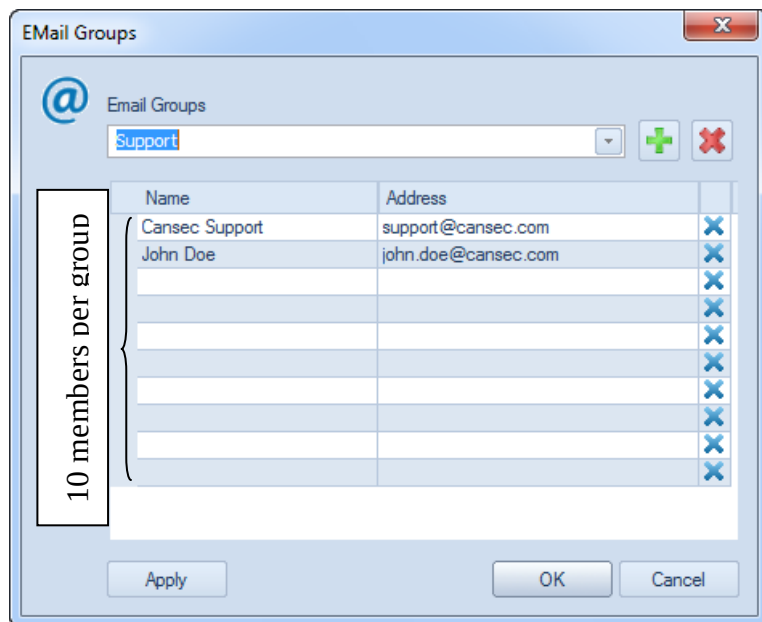


ALARM NOTIFICATIONS



Certain events or alarms from readers, inputs and outputs point can be selected to show up in the alarm queue and optionally be notified via email when the event or alarm occurs. Email notification is available only in **First Access Advanced** and uses *System Schedule* for notification scheduling.

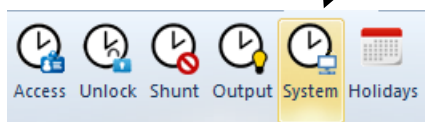
➤ Email Groups



1. Click **Email** icon  to launch Email Groups
2. Click  button
3. Enter the name for the group e.g. *Support* or *IT* or *Managers* etc...
4. Enter the name and corresponding email address for up to 10 members of each group. Click **Apply** to save changes to the current email group.
5. Click **OK** when done.

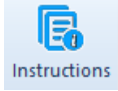
Note: Use button  to add additional email groups. Use button  to remove an email group. Use button  to remove an email address.

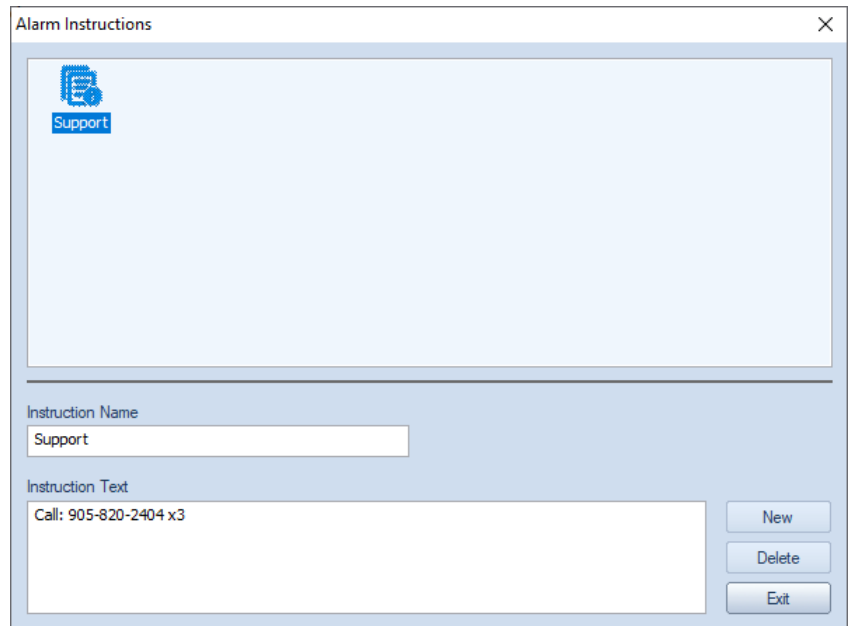
Important: Use *System Schedule* for email notification scheduling.



➤ Alarm Instructions

Instructions can be predefined to be included in the alarm queue or included with the email alarm notification. Instruction may contain contact name or phone number along with information to carry out in an event of an alarm.

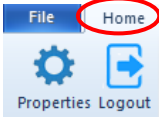
1. Click  icon to launch **Alarm Instructions** window containing a list of instructions.
2. Click **New** to create new instruction.
3. Input a name for the instruction e.g. *Support*
4. Input the instructions in the instruction text panel.
5. Click **Exit** to save the instruction and to exit.
6. Optionally, highlight any existing instruction to edit or delete it.

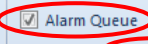


The screenshot shows the 'Alarm Instructions' window. It has a title bar with a close button. Inside, there's a 'Support' icon and a list of instructions. Below the list, there are input fields for 'Instruction Name' (containing 'Support') and 'Instruction Text' (containing 'Call: 905-820-2404 x3'). To the right of these fields are buttons for 'New', 'Delete', and 'Exit'.

Sample Alarm Notification:

If the Alarm Queue is not displayed at the bottom of the application, select Home

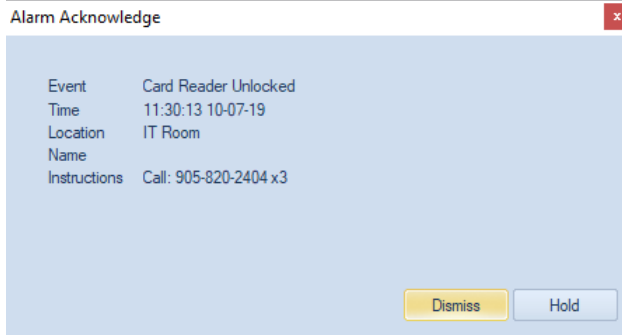
on the top menu  then from the top right corner under Window section,

select **Alarm Queue**  

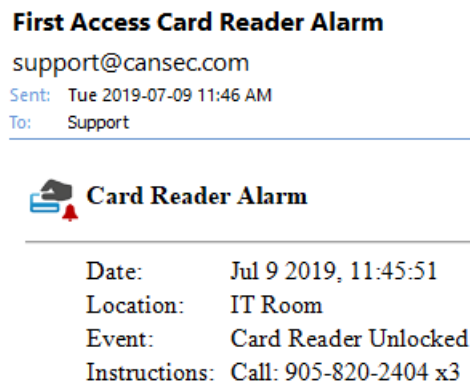
When an alarm occurs, it will be shown in the queue below

Alarm Queue					
Priority	Date	Alarm	Card	Name	Location
1	10-07-19 11:30	Card Reader Unlocked			IT Room

Double click on the event to either dismiss or hold it in the queue

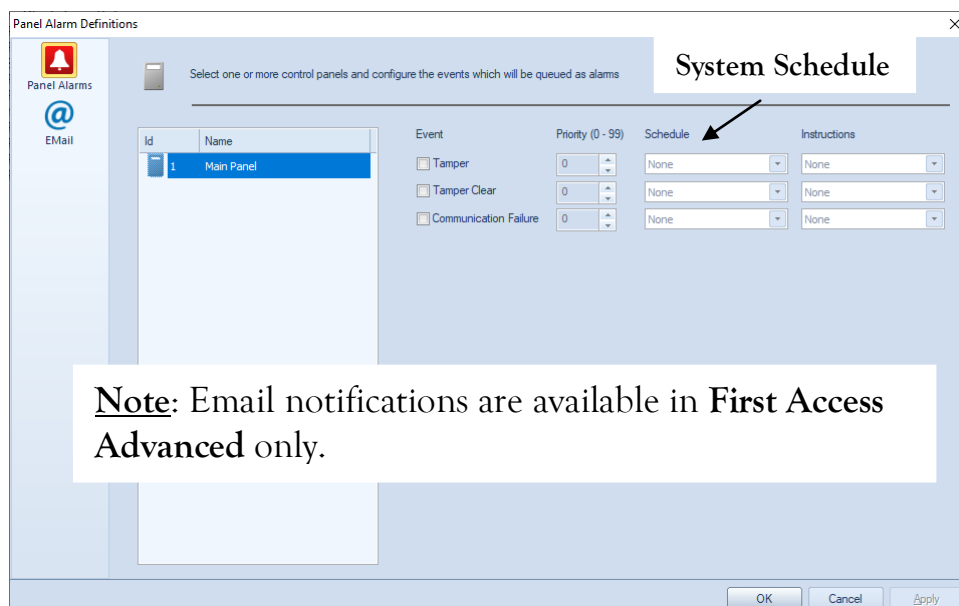


If email notification is setup then an email notification will be sent like the sample notification below.

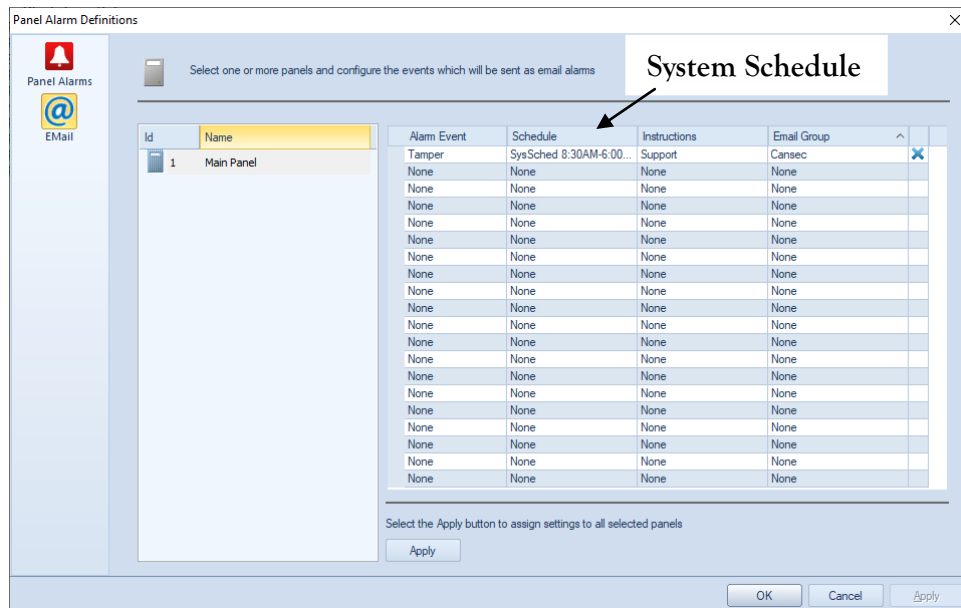


➤ Panel Alarm Notifications

1. Click **Panels** icon  to launch Panel Alarm Definitions

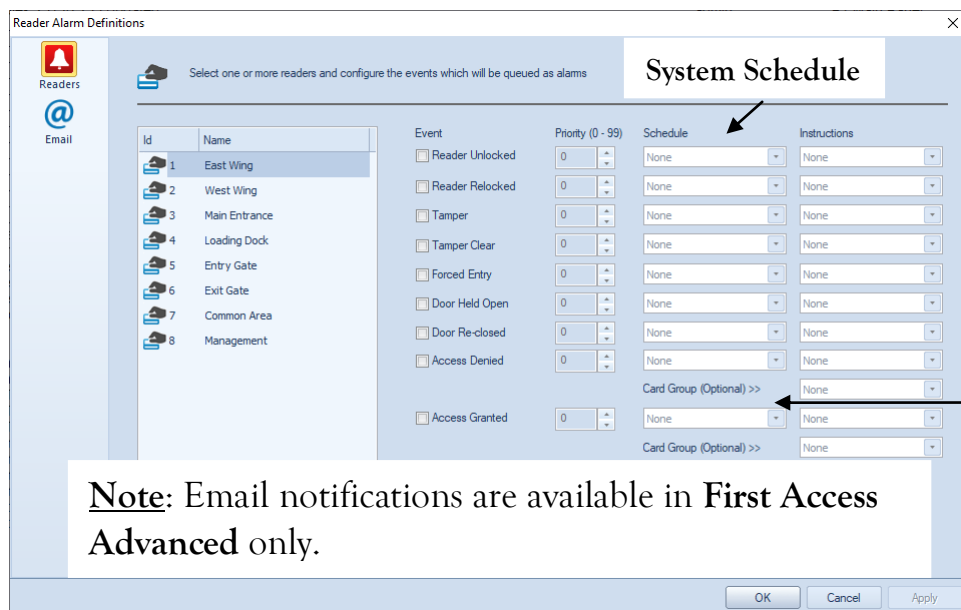


2. Select desired panel, event, priority, schedule and instruction to be displayed in the alarm queue. The event sorting priority (0 to 99) defines the order in which events are displayed in the alarm queue. (See *Alarm Queue* section)
3. Select **Email** to setup email notification. Click **OK** when done.



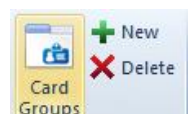
➤ Reader Alarm Notifications

1. Click **Readers** icon 



Card Filtering Option:

Notify only when certain cards access the door. Card Groups must be created.



2. Select the desired reader, event, priority, schedule and instruction to be displayed in the alarm queue. The sorting priority (0 to 99) defines the order in which events are displayed in the alarm queue.
3. Select **Email** to setup email notification. Click **OK** when done.

➤ Input Alarm Notifications

Note: Auxiliary Input and Output are available in **First Access Advanced** only.

1. Click on Inputs icon 

Note: Email notifications are available in **First Access Advanced** only.

2. Select the desired input, event, priority, schedule and instruction to be displayed in the alarm queue. The sorting priority (0 to 99) defines the order in which events are displayed in the alarm queue.

System Schedule

Select one or more inputs and configure the events which will be sent as email alarms

	Name	Alarm Event	Schedule	Instructions	Email Group
	1 Panic Button	None	None	None	None
	2 Lockout Off	Secure Alarm	None	None	None
	3 Main Entrance Unlock/Relock B...	Trouble	None	None	None
	4 Output On/Off	None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None
		None	None	None	None

Select the Apply button to assign settings to all selected devices

3. Select **Email** to setup email notification. Click **OK** when done.

➤ Output Alarm Notifications



1. Click on **Outputs** icon

Note: Auxiliary Input and Output are available in **First Access Advanced** only.

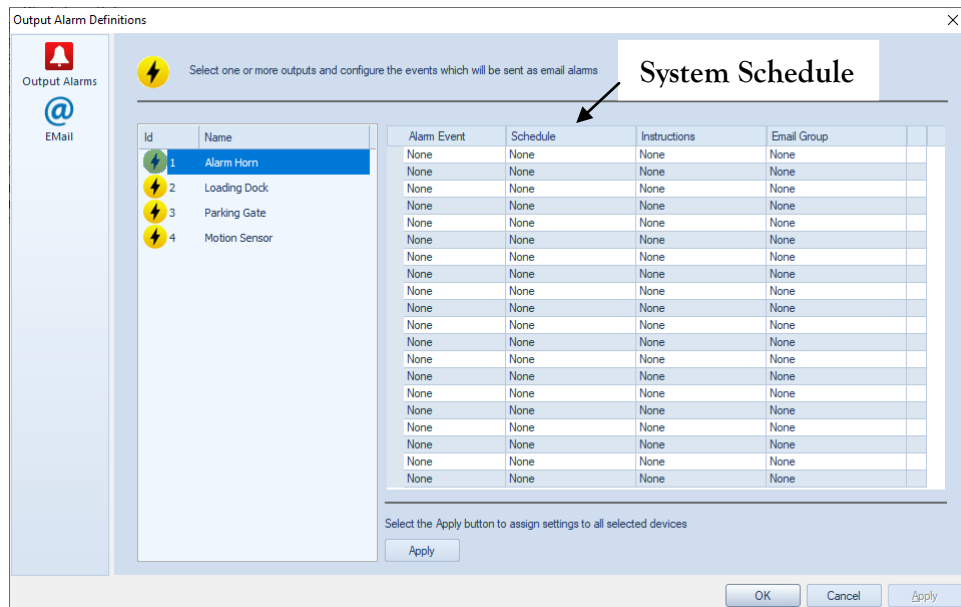
Output Alarm Definitions

Select one or more outputs and configure the events which will be queued as alarms

Id	Name	Event	Priority (0 - 99)	Schedule	Instructions
1	Alarm Horn	☐ Output Off	0	None	None
2	Loading Dock	☐ Output On	0	None	None
3	Parking Gate				
4	Motion Sensor				

Note: Email notifications are available in **First Access Advanced** only.

2. Select the desired output, event, priority, schedule and instruction to be displayed in the alarm queue. The sorting priority (0 to 99) defines the order in which events are displayed in the alarm queue.



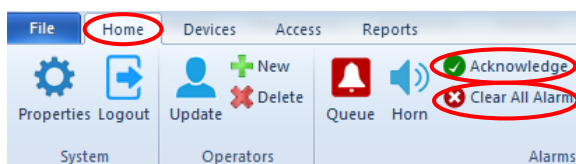
3. Select **Email** to setup email notification. Click **OK** when done.

ALARM QUEUE

Alarm queue is displayed at the bottom of the application. It shows all the alarms related to readers, inputs and outputs

Alarm Queue					
Priority	Date	Alarm	Card	Name	Location
2	28-09-16 17:49	Card Reader Unlocked			Front Door
1	28-09-16 17:49	Card Reader Unlocked			IT Room
1	28-09-16 17:49	Output On			Alarm Horn

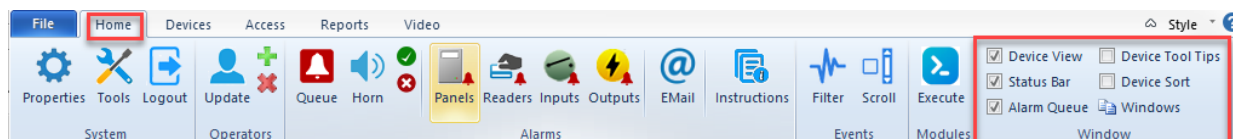
Individual alarm entry in the queue can be cleared or acknowledged by double clicking on the selected entry. Selected individual alarm entry or all entries can also be cleared by using the top menu buttons  **Acknowledge** and  **Clear All Alarms** respectively.



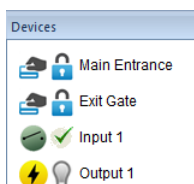
Alarm Horn can be enabled or disabled by clicking the icon  to toggle it on or off

Alarm Queue can be enabled or disabled by clicking the icon  to toggle it on or off

APPLICATION WINDOWS



- Select check box ☒ **Device View** to show or hide **Device View** window



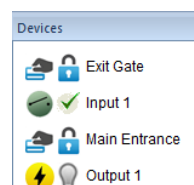
- Select check box ☒ **Status Bar** to show or hide **Status Bar** window



- Select check box ☒ **Alarm Queue** to show or hide **Alarm Queue** window

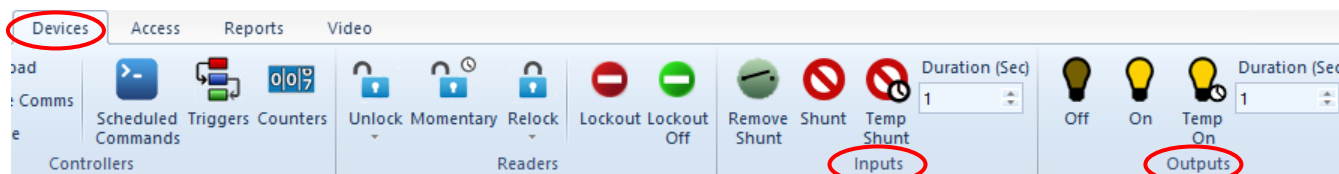
Alarm Queue					
Priority	Date	Alarm	Card	Name	Location
2	28-09-16 17:49	Card Reader Unlocked			Front Door
1	28-09-16 17:49	Card Reader Unlocked			IT Room
1	28-09-16 17:49	Output On			Alarm Horn

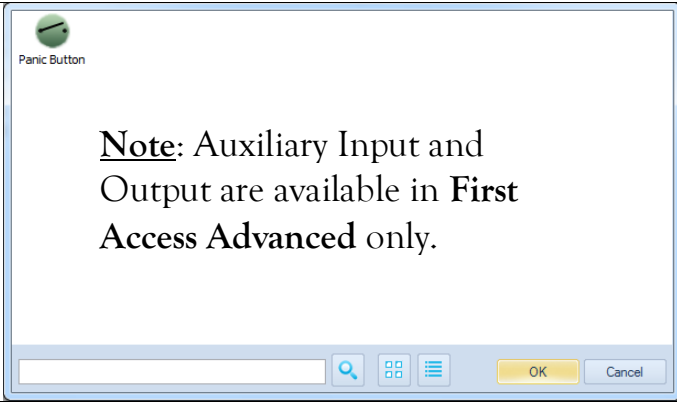
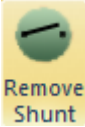
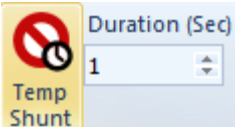
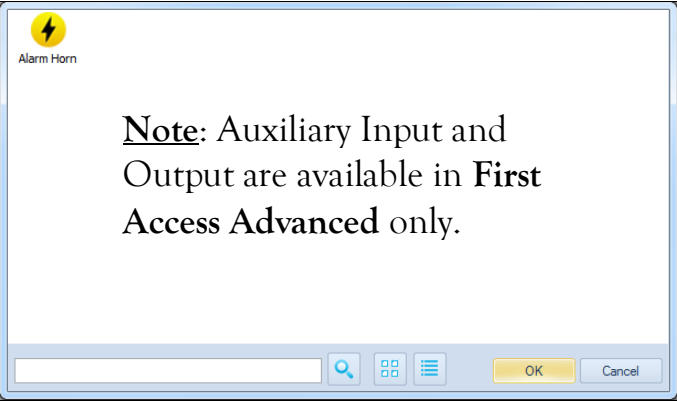
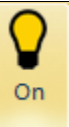
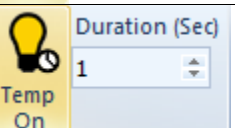
- Select check box ☒ **Device Sort** to sort devices in alphabetical order



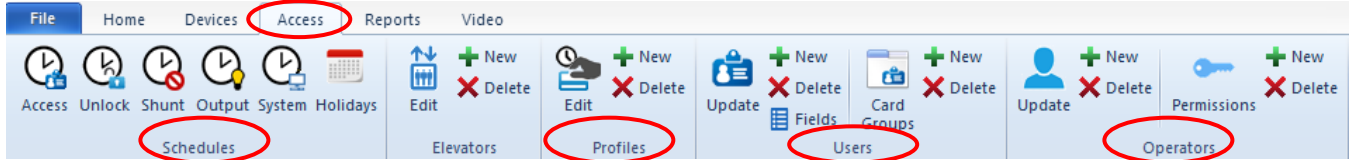
INPUT AND OUTPUT COMMANDS

Note: Auxiliary Input and Output are available in **First Access Advanced** only.



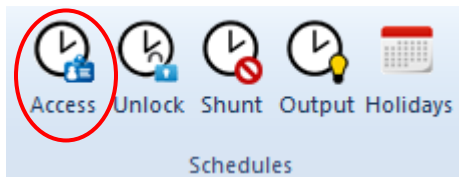
Input Points		<u>Note:</u> Sample input point named <i>Panic Button</i>
	Click and select an input point from the list to remove it from being shunted. This allows the input events to be processed normally by the controller or panel.	
	Click and select an input point from the list to shunt it. This instructs the controller to ignore the input events.	
	Click and select an input point from the list to temporarily shunt it for the entered duration in seconds. This instructs the controller to temporarily ignore the input events for the entered duration.	
Output Points		<u>Note:</u> Sample output point named <i>Alarm Horn</i>
	Click and select an output point from the list to turn it off.	
	Click and select an output point from the list to turn it on.	
	Click and select an output point from the list to temporarily turn it on for the entered duration in seconds.	

Step 4. Schedules, Profiles, Users and Operators



Select **Access** from the top menu.

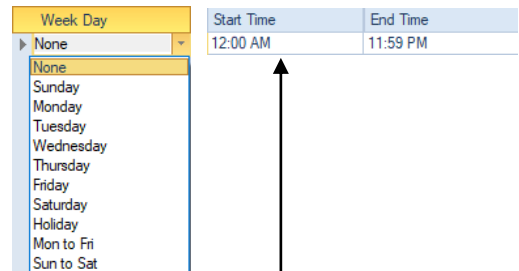
 ACCESS SCHEDULES



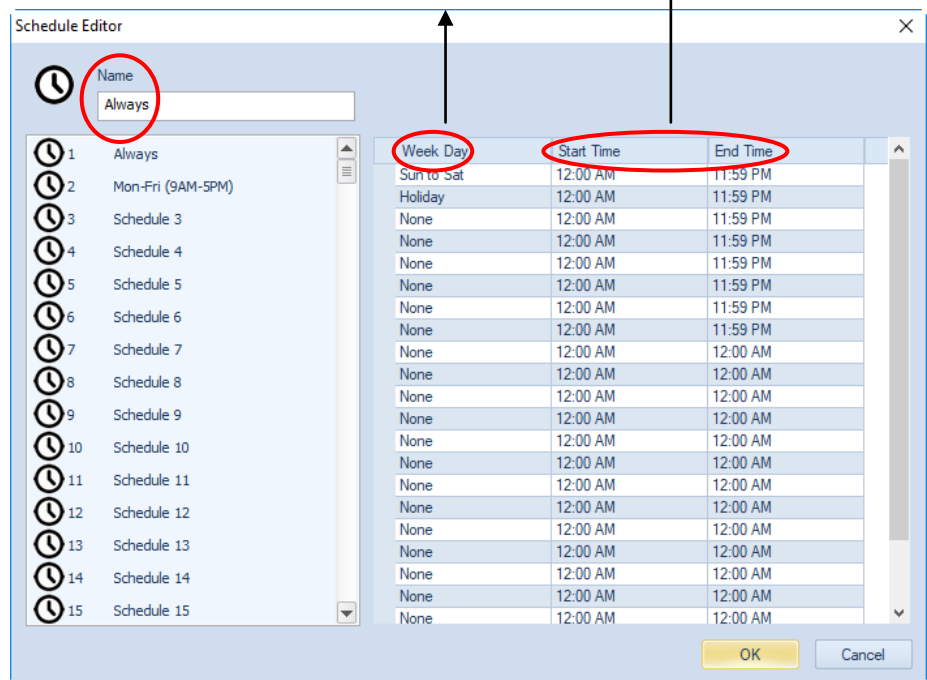
Note: There are 24 available intervals shared between weekdays (7 days from Sunday to Saturday) and a holiday (1 day) for a total of 8 days. Several intervals can be defined within a day, e.g. Monday 9:00AM to 12:59PM and Monday 1:00PM to 5:00PM. More than 3 intervals can be defined within a day as long as the number of intervals for the 8 days (Mon to Sun and Holiday) does not exceed 24.

Access schedules specify when cardholders can use their credentials to access a door.

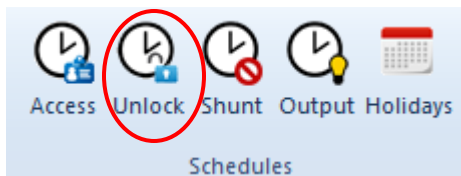
1. Click the **Access Schedule** icon.
2. Select one of the 255 available access schedules.



3. Enter a name for the access schedule, e.g. *24/7* or *Always*.
4. Select an option for the Week Day. Double click on hour, minutes and period (AM or PM) to modify times accordingly. Click



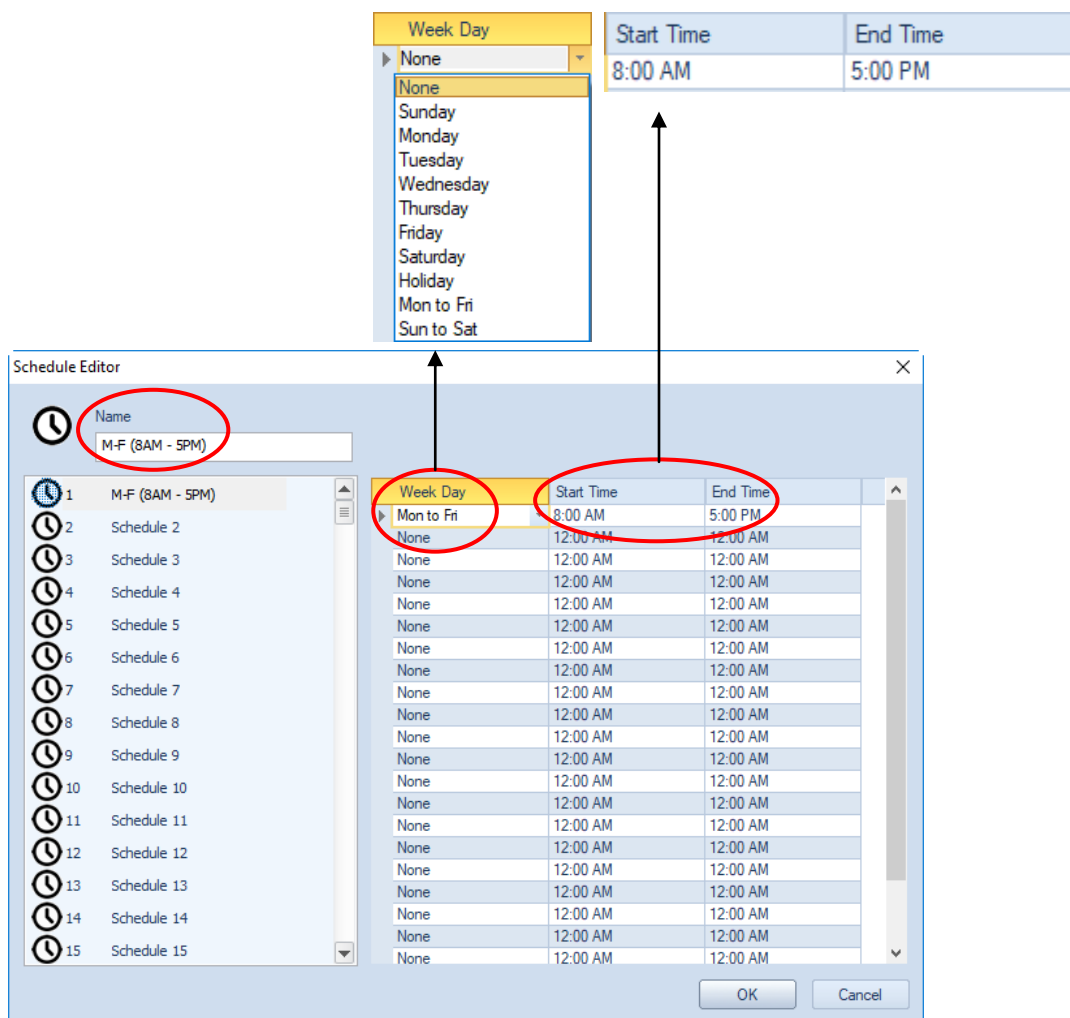
UNLOCK SCHEDULES



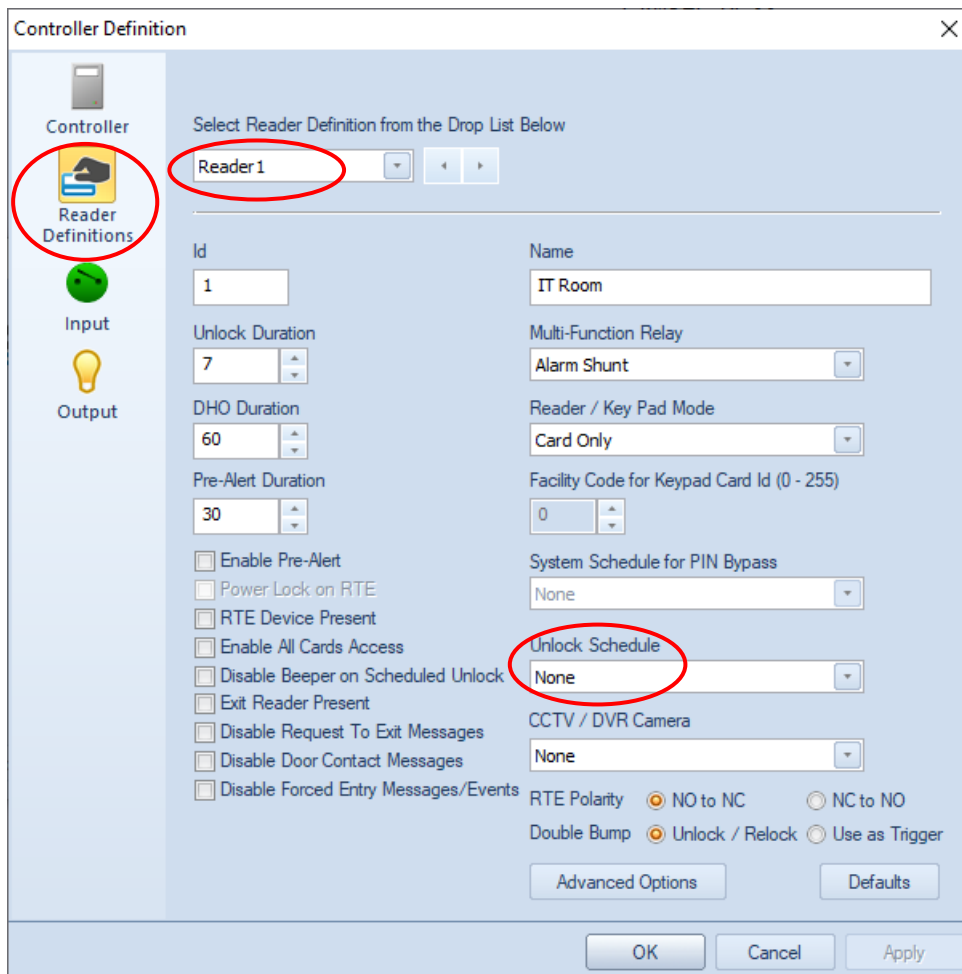
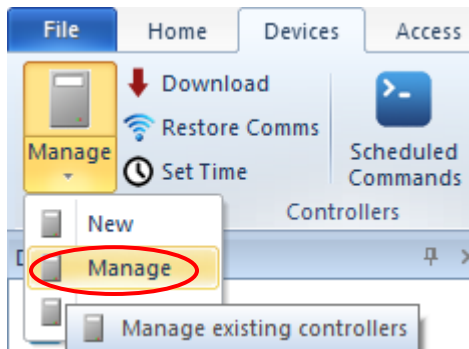
Unlock schedules are used to automatically unlock and relock a door at specified times.



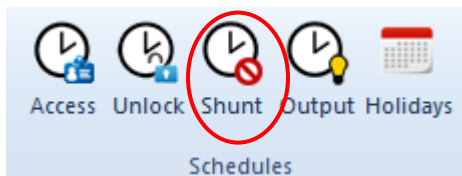
1. Click on the Unlock icon.
2. Select one of the 255 available unlock schedules.
3. Enter a name for the access schedule, e.g. M-F 8AM-5PM.
4. Select the day of the week. Double click on hour, minute and period (AM or PM) to modify times accordingly.



5. To assign an unlock schedule to a door, select **Devices>Manage** and select a desired panel. Select **Reader Definition** and select an unlock schedule to assign to that door.



6. Click **OK** when done.

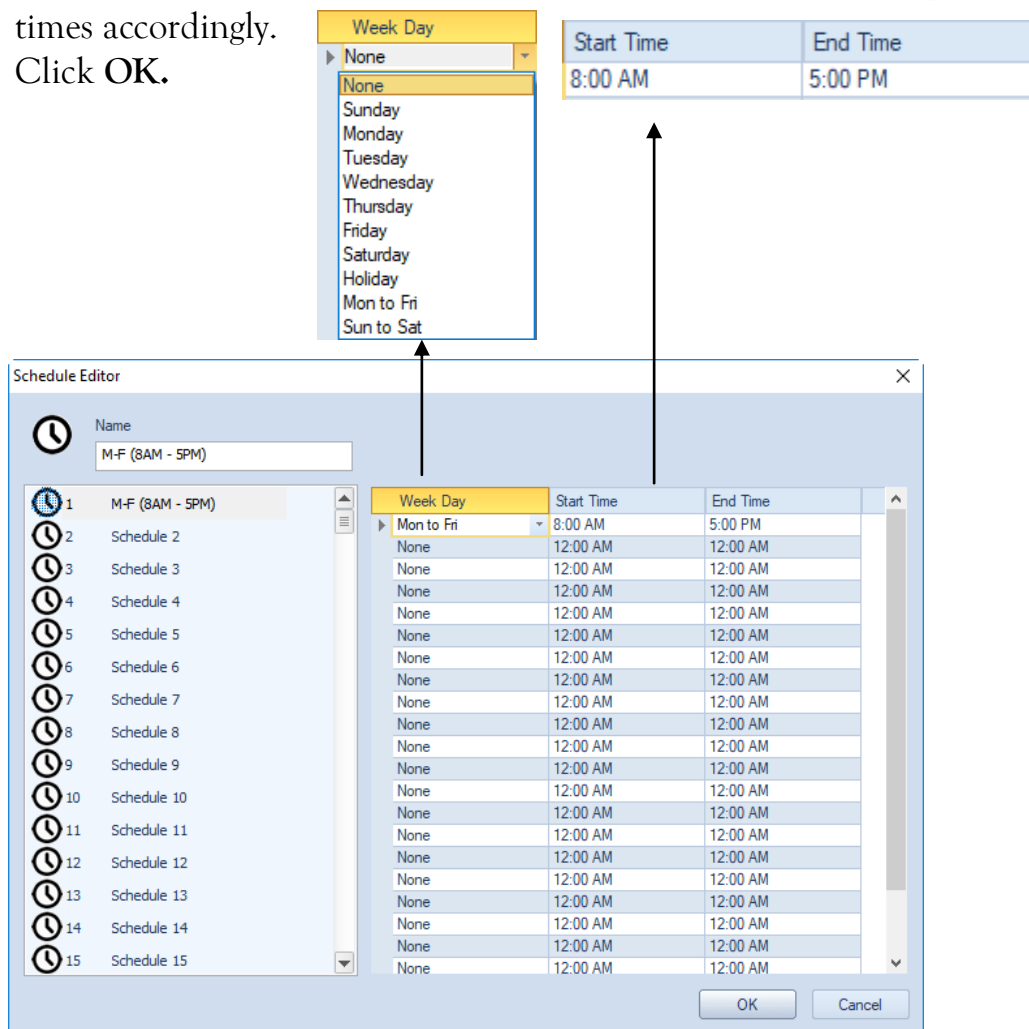


Note: Available in **First Access Advanced** only.

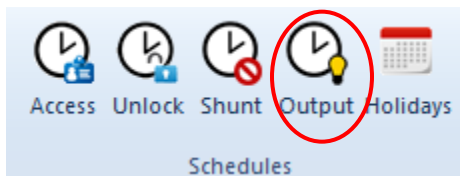
Shunt schedules are used to instruct the controller or the panel when to process and when to ignore input point events.



- Click on the Shunt icon 
- Select one of the 255 available shunt schedules.
- Enter a name for the shunt schedule, e.g. M-F (8AM-5PM)
- Select the day of the week. Double click on hour, minute and period to modify times accordingly.
- Click **OK**.



OUTPUT SCHEDULES

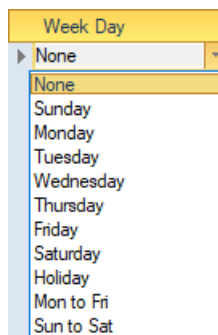


Note: Available in **First Access Advanced** only.

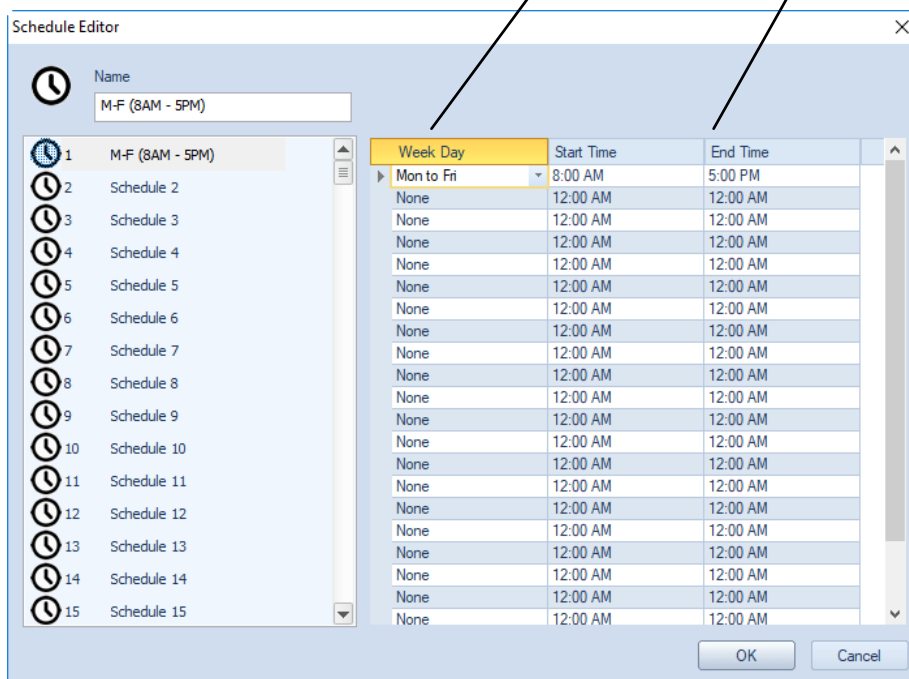
Output activation schedules are used to activate output points automatically during specified times.



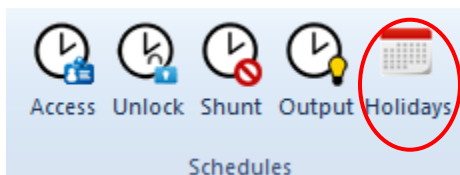
1. Click on the Output icon
2. Select one of the 255 available shunt schedules.
3. Enter a name for the Output schedule, e.g. M-F (8AM-5PM)
4. Select the day of the week.
Double click on hour, minute and period to modify times accordingly.
5. Click **OK**.



Start Time	End Time
8:00 AM	5:00 PM

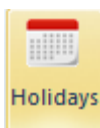


HOLIDAY SCHEDULES

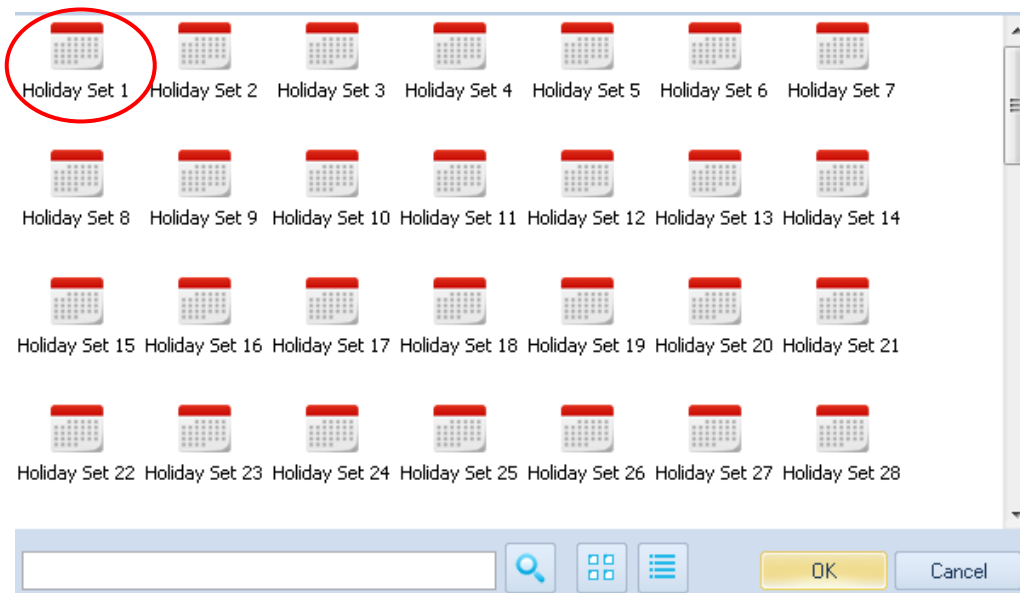


Note: A Holiday is not restricted to an individual day. It can start at any time within the day, and end in the same day or a different day at a different time. For example, consider the case of a company which shuts down for a week at noon on December 24th until January 2nd of the New Year. This would be accommodated using a holiday start date of December 24th at 12:00PM until January 2nd at 12:00AM.

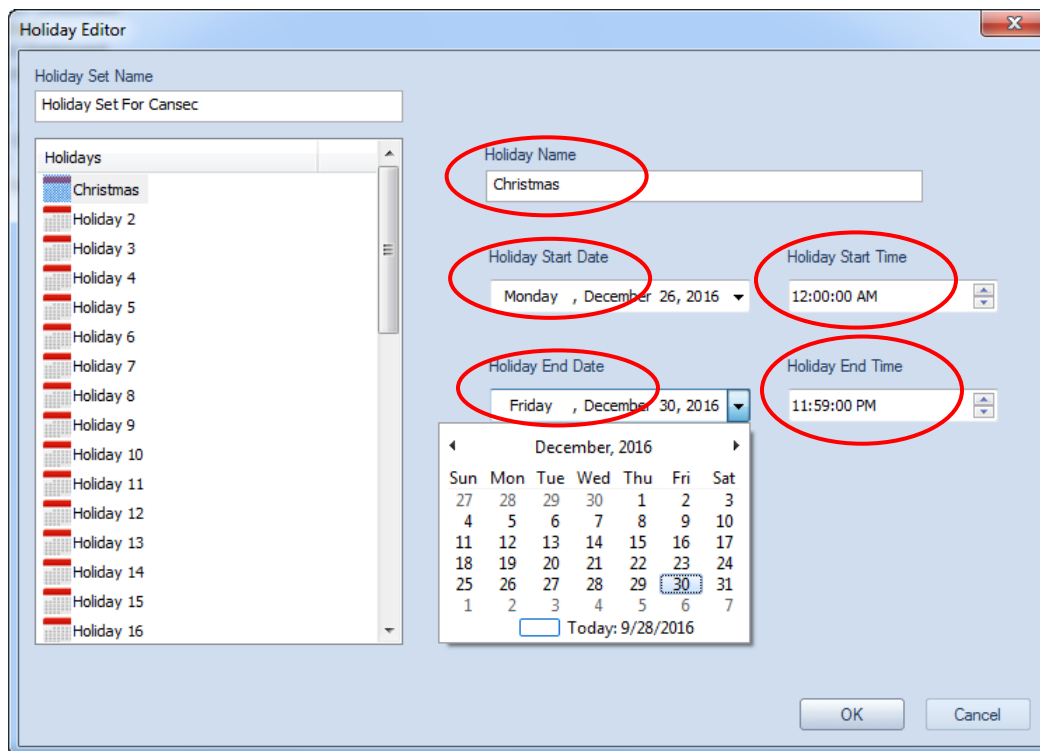
Holidays can be defined so that schedules like door unlock schedules and other schedules do not take effect on days which are holidays. Holidays can be optionally grouped into different sets for ease of assignment to different controllers, or they all can share the same set. To create a new holiday:



1. Click the **Holiday** icon.
2. Double click on one of the 100 available holiday sets.



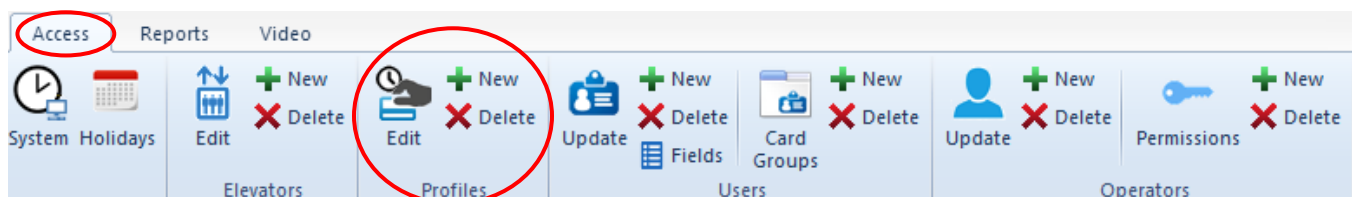
3. Enter a name for the **Holiday Set Name** or leave as is. Enter a name for the **Holiday Name**, e.g. *Christmas*.



4. Use the arrows to select the month and the desired date for **Holiday Start Date** and enter the time for the **Holiday Start Time**.
5. Use the arrows to select the month and the desired date for **Holiday End Date** and enter the time for the **Holiday End Time**. Click OK.

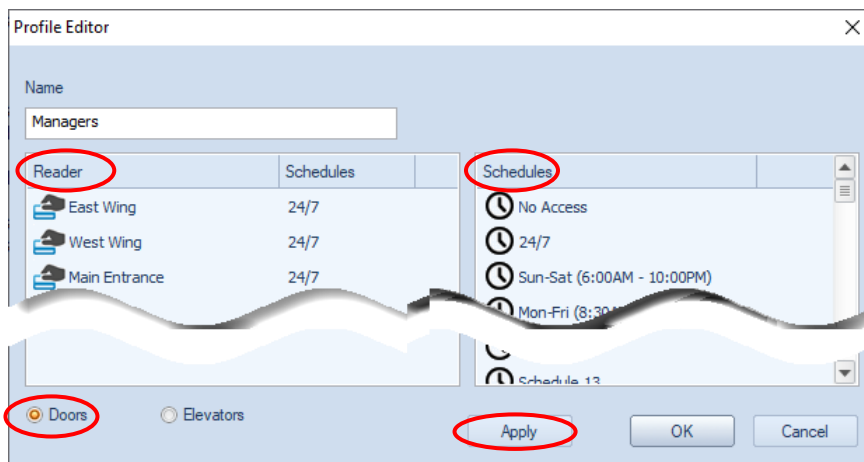
ACCESS PROFILES

Note: Operator permissions are available in **First Access Advanced** only.

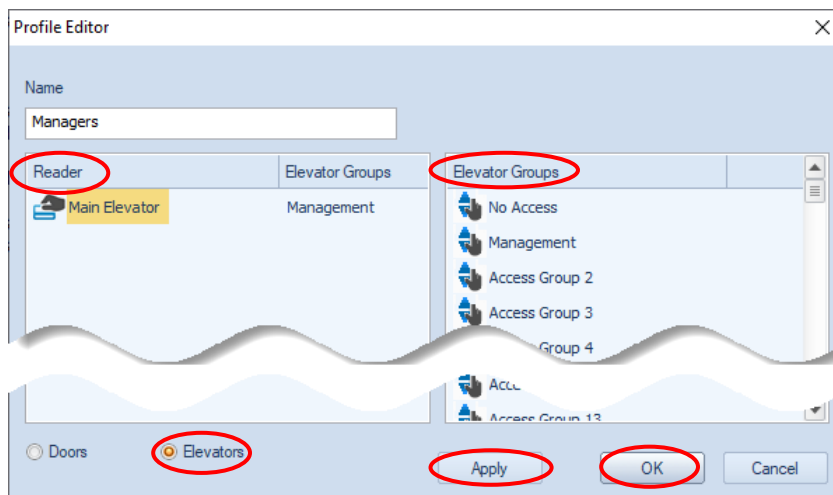


Access profiles specify which doors a group of cardholders can access, and the time during which access will be granted at each door. To create a new Access Profile:

1. In **Profiles** section, click the **+New** icon. 
2. Enter a name for the profile, e.g. Managers.



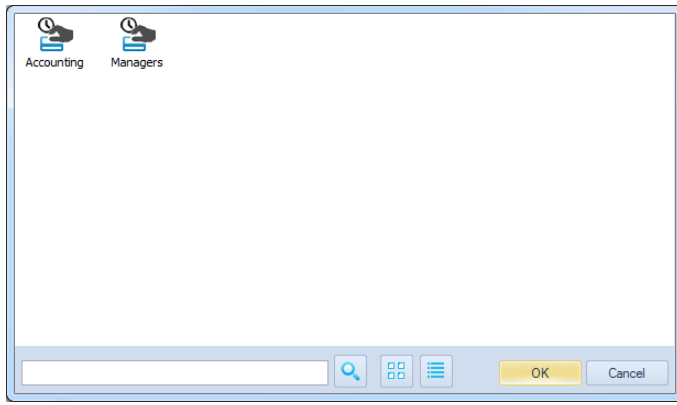
3. For **Doors**, select a reader on the left panel and select a schedule on the right panel to assign to the reader. Click **Apply**. Repeat the same step for other reader(s) if necessary. If there is no elevator then skip steps related to elevator and click **OK** to finish.
4. For **Elevators**, select the elevator on the left panel and select an elevator group on the right panel to assign to the elevator. See *Elevator section in this document for more information*



5. Cardholders who belong to this profile will only be able to access the readers or doors during the times specified in the associated access schedule. Likewise, if elevator is assigned then cardholders in this profile can only access elevator floors specified in that elevator group e.g. *Management*. See **Elevator** section for more information about elevator group and how to define elevator groups.
6. Click **OK** when done.

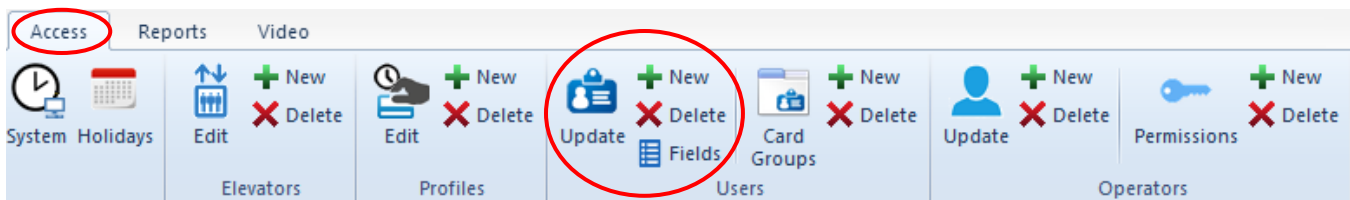


To modify or delete a profile select **Edit** or **Delete** respectively. Select a desired profile to be modified or deleted and click **OK**.



Note: To delete a profile, all users of that profile must be assigned to a different profile before it can be deleted. See **Cardholder Report** section for information about assigning or migrating multiple users to a different profile.

ADD CARDHOLDERS AND CARD GROUPS



➤ Card Holders

Note: Operator permissions are available in **First Access Advanced** only.

1. In the **Users** section, click the **+New** icon. beside the update button.

The **User Definition** dialog box contains the following elements:

- Left Sidebar:** Identification (selected), ID, Dates, Access, Fields, Notes, Privilege.
- User Information:** First Name, Last Name, Keypad PIN Number (Card + PIN Mode) (00000000).
- User Options:**
 - ☐ Handicapped
 - ☐ PIN Bypass
 - ☐ Lockout Bypass
 - ☐ Interlock / APB Bypass
 - ☐ AD Service Exempt
- Photo:** A placeholder image for the user's photo, with an **Import Photo** button below it.
- Buttons:** OK, Cancel, Apply.

Applicable for CARD + PIN only. Ignore if not using keypad for CARD + PIN

Available in First Access Advanced only. Import with pre-taken picture

Active Directory attribute for AD queries must be entered for AD Import button and input field to appear or otherwise hidden

Enter the Active Directory attribute for AD queries

If applicable, use AD Import to import all attributes e.g. First Name, Last Name, Department, and Phone Number etc... of a user that will be mapped to the user fields and other fields. In this example, we use the email as a unique attribute of the user to query and import all other attributes of that user.

2. If Card + PIN is used, create/enter the PIN number for this card. To bypass PIN requirement for certain day and times, create a system schedule then select that bypass schedule. *In this mode, the card must be presented followed by the PIN number followed by #.*

Reader / Key Pad Mode

Card + PIN

Facility Code for Keypad Card Id (0 - 255)

0

System Schedule for PIN Bypass

None

- Handicapped: The door operator will be energized when this cardholder swipes his/her credential. Note: The door operator must be installed and hooked up to the MAP controller using the Multi-Function relay which must be set to Handicap Operator mode.
- PIN Bypass: This cardholder is exempted from entering the PIN when Card + PIN is required
- Lockout Bypass: This cardholder is granted access when reader is in lockout mode
- Interlock/APB Bypass: This cardholder is granted access when reader is in interlock or anti-passback mode
- AD Service Exempt: This cardholder is exempted from Active Directory Access Service. See **Active Directory Access Service** section for more information.

3. In the **ID** tab, select a credential from the drop-down list. Select a credential format. For **Raw Wiegand** present the credential to the enroller and click **Enroll**. For other Wiegand formats simply enter the system/facility code and the credential number in the field **System/Facility Code** and **ID Number** respectively.

User Definition

Select one of the 5 credentials from the drop list below

Credential 1

Credential Format

- ☐ Raw Wiegand
- ☐ 26 Bit Wiegand
- ☒ 37 Bit Cansec
- ☐ 48 Bit Corporate 1000
- ☐ 35 Bit Corporate 1000
- ☐ 36 Bit Keyscan C15001
- ☐ 37 Bit AMAG
- ☐ 36 Bit Verex

System / Facility Code

1603

ID Number

08471

Raw Format

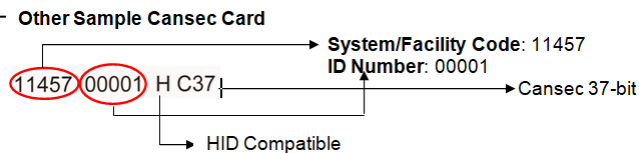
Bit Count: 0 Hex Wiegand Data: 0000000000000000

Enroll Delete

OK Cancel Apply

A person may possess up to 5 credentials or an apartment with a family of 5 members

If using keypad for entering card number known as PIN number only (not Card + PIN) then enter the System/Facility System code of the keypad and enter the PIN number you wish to assign to this user in the field ID Number. *Please follow keypad's manual to program they keypad with a system/facility code for use with Cansec controllers.*



4. In the **Dates** tab, select the dates and times for the credential to be automatically validated and automatically expired. *Example, you may give a guest a card or a PIN code which you can set it to be validated and expired at certain date and time.*

User Definition

Credential Activation Date Range

Valid From Date and Time

5/26/2016 12:00:00 AM

Until Date and Time

1/ 1/2050 12:00:00 AM

January, 2050

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today: 5/26/2016

OK Cancel Apply

5. In the **Access** tab, select a **Credential Status** and select an **Access Profile** previously created. For new credentials, set the credential status to **Active**. Credentials that have status set to **Inactive**, **Lost**, **Stolen** or **Destroyed** will not be granted access to any door.

The screenshot shows the 'User Definition' window with the 'Access' tab selected. The 'Access Information' section contains three dropdown menus: 'Credential Status' (set to 'Active'), 'Primary Access Profile' (set to 'Classified Staff'), and 'Select a Secondary Access Profile' (set to 'Harbor Properties'). Below these is a list of 'Secondary Profiles' including 'Creative', 'Facilities', and 'Harbor Properties'. On the right side, there are buttons for 'Insert Profile', 'Move Profile Up', 'Move Profile Down', 'Remove Profile', and 'Show Final Access'. At the bottom, the 'OK' button is circled in red.

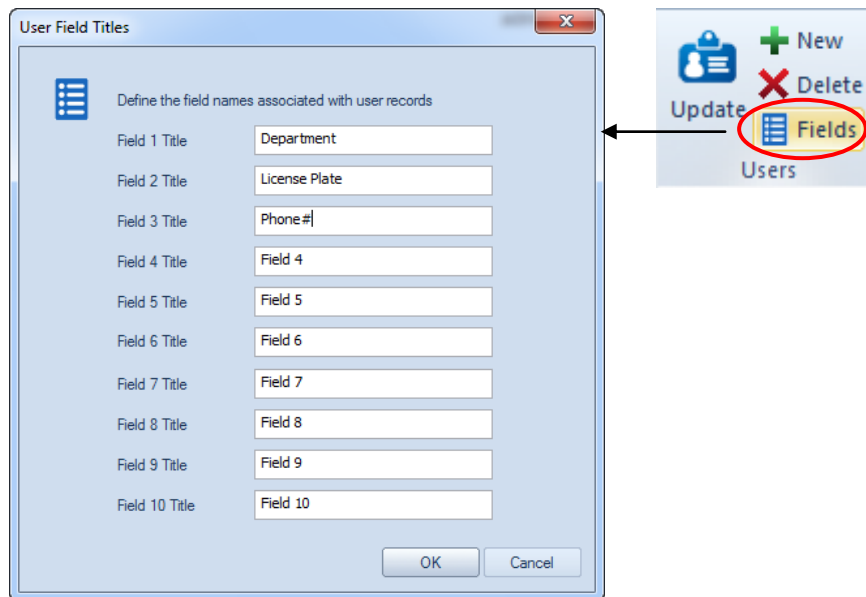
If necessary select additional access profiles as secondary access profiles to allow a cardholder additional access to certain doors.

Access profiles are processed in priority sequence starting with primary access profile followed by other sequential secondary access profiles that can be moved up/down.

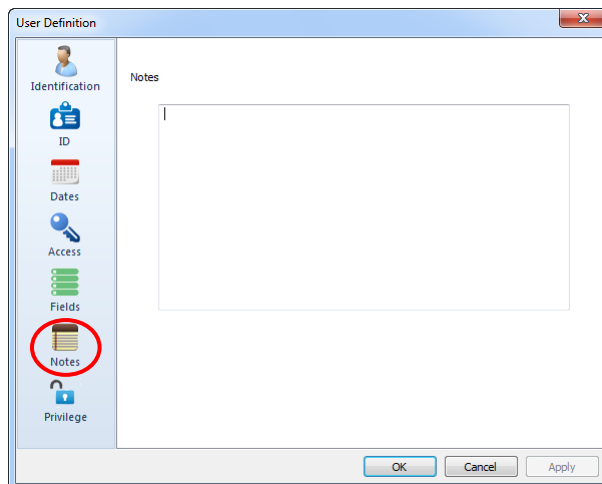
6. In the **Fields** tab, enter optional information in the 10 available fields, e.g. *Phone #, Parking lot #, Car license plate*, etc.

The screenshot shows the 'User Definition' window with the 'Fields' tab selected. The 'Discretionary Data' section contains 10 text input fields labeled 'Field 1' through 'Field 10'. At the bottom, the 'OK' button is circled in red.

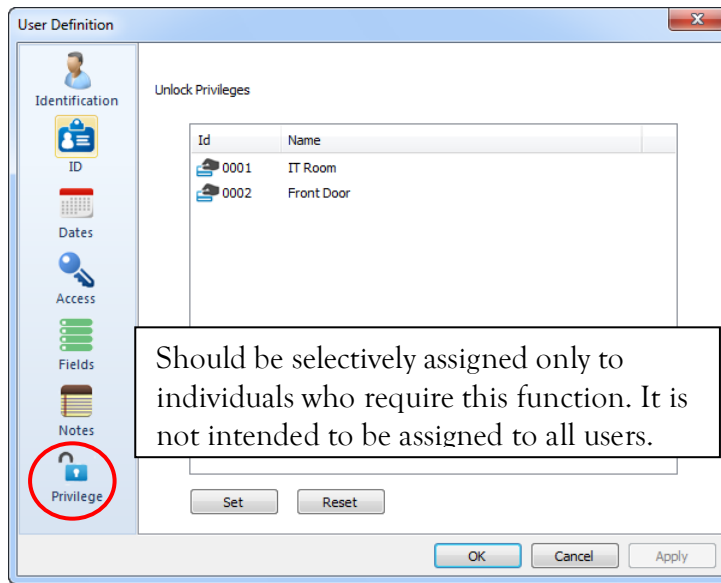
Note: The field titles e.g. Field1, Field2 etc... can be renamed as desired by selecting **Fields** from the **Users** menu and modify the name of those fields accordingly.



7. In the **Notes** tab, enter optional notes.



8. In the **Privilege** tab, optionally select door(s) that this cardholder is entitled to toggle between locked and unlocked state when their credential is double swiped at the card reader. Click **Set**, after doors have been selected, to assign the privilege or click **Reset** to clear the privilege.



Important: The double-swipe privilege is optional and should be assigned only to privileged cardholders e.g. Managers, Supervisors.

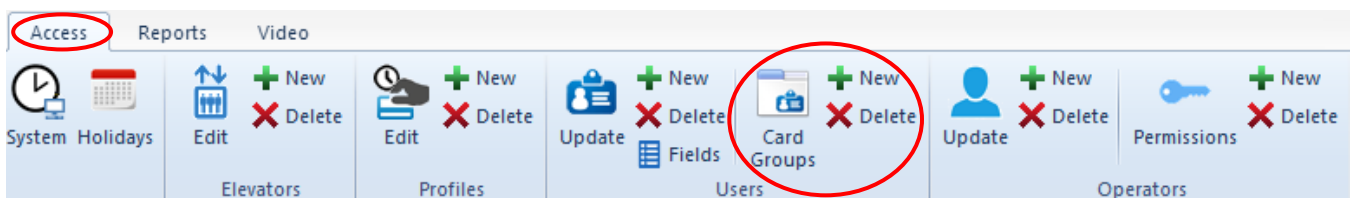
Note: Double swipe will unlock the door in a maintained state and double swipe again will relock the door. Single swipe will momentarily unlock the door for the duration that is set in the unlock-time setting of that door.

9. Click OK. Confirmation message(s) will be displayed in the **Events** panel.

Time	Date	Event	Name	Bit Count	Credential	Operator	Location
11:15:42	08-04-19	Card Validated, Schedule 2	Support, Cansec	37	1603:08471	admin	IT Room
11:15:42	08-04-19	Card Validated, Schedule 2	Support, Cansec	37	1603:08471	admin	Main Entrance

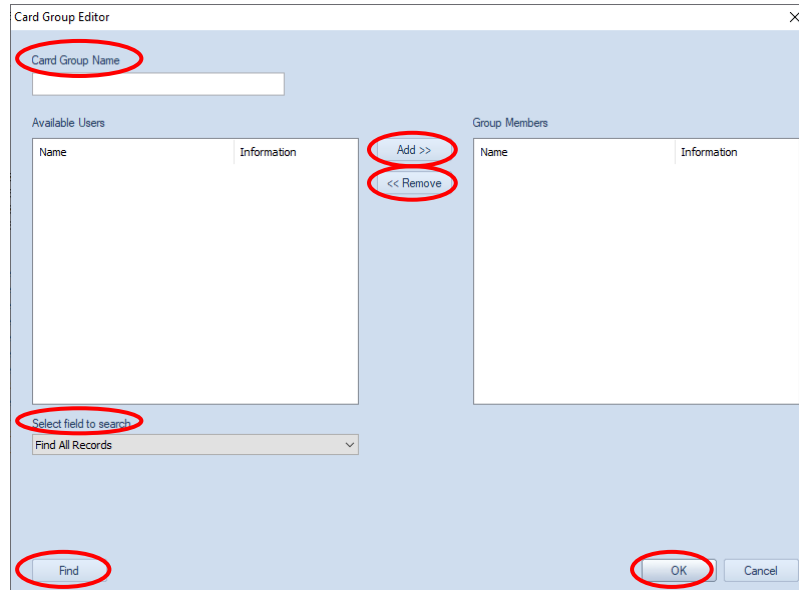
➤ Card Groups

Card groups provide an option to group a number of cardholders together in a group which can be used in the unlock schedule or in the trigger feature (see trigger section for more info). It is used to determine which group can perform certain actions. There are 100 card groups per controller and 75 cardholders per group. All controllers share the same groups. See trigger section for more information



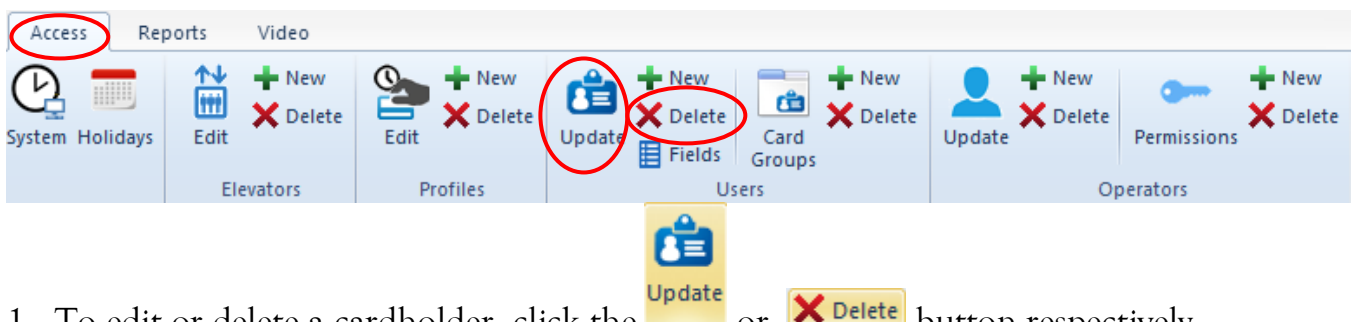
Note: Operator permissions are available in **First Access Advanced** only.

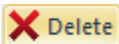
1. Click  beside the **Card Groups** button



2. Enter a name for the group e.g. Managers etc...
3. Find certain cards or all cards using the filter then add those cards to the groups. Click **OK** when done.
4. If more groups are required then repeat the same steps.
5. Select Card Groups button to edit or select Delete button to delete.

SEARCH, EDIT AND DELETE CARDHOLDER



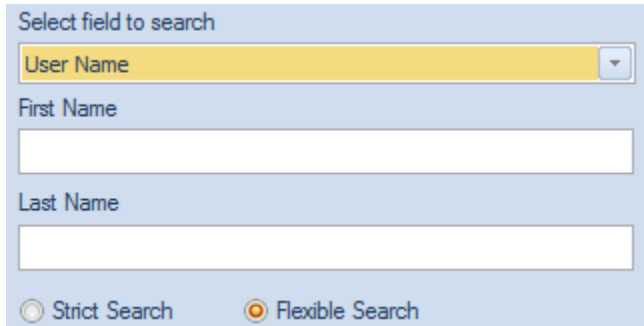
1. To edit or delete a cardholder, click the  or  button respectively.

To delete multiple cardholders see **Cardholder and Credential Report** or **Bulk Cardholder Deletion** section for more information

2. Select a desired option to search for e.g. *All Records*, *User Name* etc....

3. To search records by Credential ID select **Credential Id Number**. If only *Facility Code* is entered then the result will be all credentials having that facility code. Similarly, if only *Id Number* is entered then the result will be all credentials having that *Id Number*. However, if both *Facility Code* and *Id Number* are entered then the result will just be one unique credential having that *Facility Code* and *Id Number*

4. To search records by user name select **User Name** and enter either First Name or Last Name or both to search.

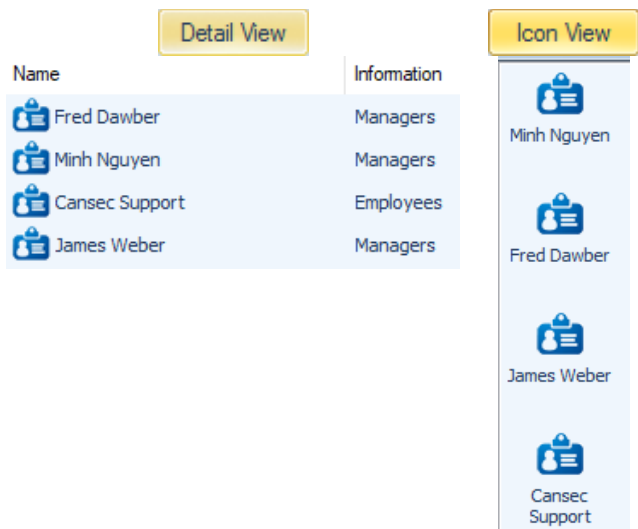


The search form is titled "Select field to search". It features a dropdown menu with "User Name" selected. Below the dropdown are two text input fields labeled "First Name" and "Last Name". At the bottom, there are two radio buttons: "Strict Search" (unselected) and "Flexible Search" (selected).

Strict Search: Requires full or complete information to be entered e.g. John not Jo will search for all first names having John. Option applies to both First and Last Name.

Flexible Search: Allows partial information to be entered e.g. Jo instead of John will search for all first names having Jo as the first 2 characters (John, Joe etc...). Option applies to both First and Last Name.

5. Results can be viewed in either detailed mode  or icon mode 



This block shows two side-by-side views of search results. The left view, titled "Detail View", shows a table with two columns: "Name" and "Information". The right view, titled "Icon View", shows a vertical list of results, each with a user icon and a name.

Name	Information
Fred Dawber	Managers
Minh Nguyen	Managers
Cansec Support	Employees
James Weber	Managers

The "Icon View" displays the same data as a vertical list of icons and names: Minh Nguyen, Fred Dawber, James Weber, and Cansec Support.

6. To edit a record, select it and click button 

- To search by access profile, select **Access Profile** and select a desired profile to search for e.g. *Managers, Employees etc...* The result will be all credentials that belong to that selected profile.

Select field to search

Access Profile

Access Profile Name

Employees

Icon View

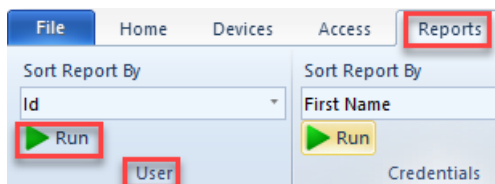
Search

Edit

Done

➤ Bulk Cardholder Deletion

To delete multiple cardholders select Report, under User section select Run



See **Cardholder and Credential Report** section for more information

Select all or desired records then right click to display a pop-up menu. Select “Delete Selected Users”.

Pin	User Id	First Name	Last Name	Validate	Void	Status	Profile	Position	Department
00000000	0010000865	D		07-06-22 00:00	01-01-50 00:00	Active	CCA		Resident Care
00000000	0010000931	M		07-06-22 00:00	01-01-50 00:00	Active	Housekeeping		Housekeeping
00000000	0010002415	M		07-06-22 00:00	01-01-50 00:00	Active	Doctors	Dr Vermaak	Doctor
00000000	0010002416	M		07-06-22 00:00	01-01-50 00:00	Active	Dietary		Dietary
00000000	0010002417	M		07-06-22 00:00	01-01-50 00:00	Active	Switch board		Switch board
00000000	0010002418	K		07-06-22 00:00	01-01-50 00:00	Active	Maintenance		Maintenance
00000000	1654631831	C		07-06-22 00:00	01-01-50 00:00	Active	Managers		
00000000	1660312898	Test	Card	12-08-22 00:00	01-01-50 00:00	Inactive	No Access		

Assign Validation Date

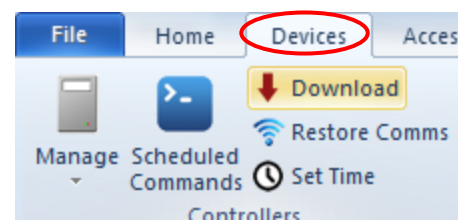
Assign Expiration Date

Assign Access Profile

Void Selected Users

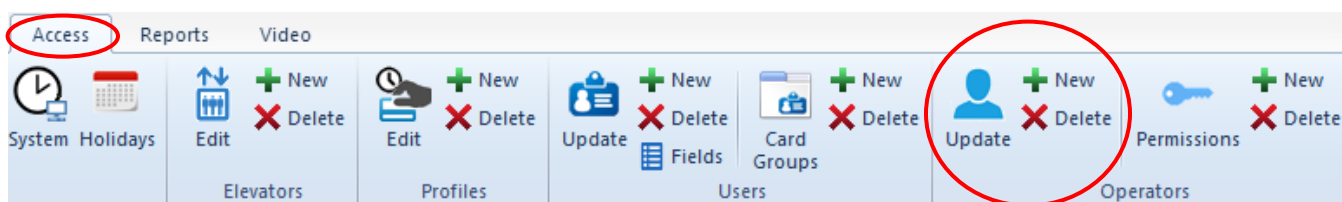
Delete Selected Users

Note: Communication must be established between the software and controller for the modified or deleted user record to be updated from the controller. If there is no communication when the modification or deletion is performed, the user record will remain in the controller database. When communication is resumed, a manual download from the software is required to update the controller again.



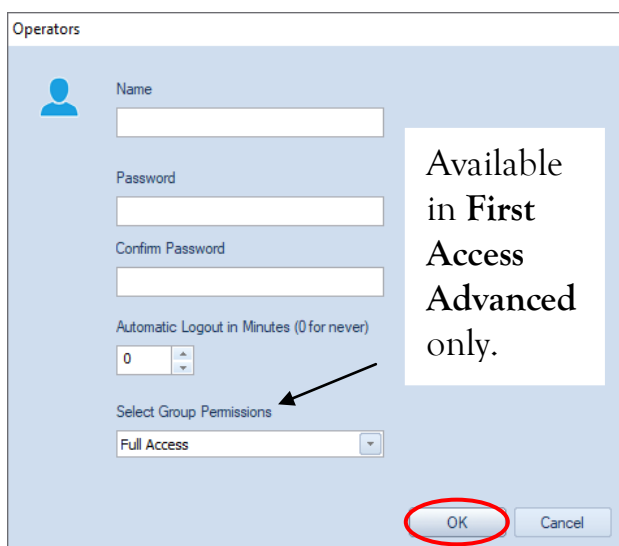
OPERATOR PROFILES

Note: Operator permissions are available in **First Access Advanced** only.



Operators are personnel who are authorized to login and manage the software and controllers or panels.

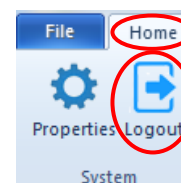
1. In the **Operators** section, click the **+New** icon  to create new operator.



There is a default operator named *admin* and the default password is *admin*. The default *admin* has full access to the software.

In *First Access Express*, every operator has full access to the software.

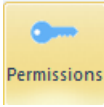
Note: Manual logout can be done by clicking on logout button

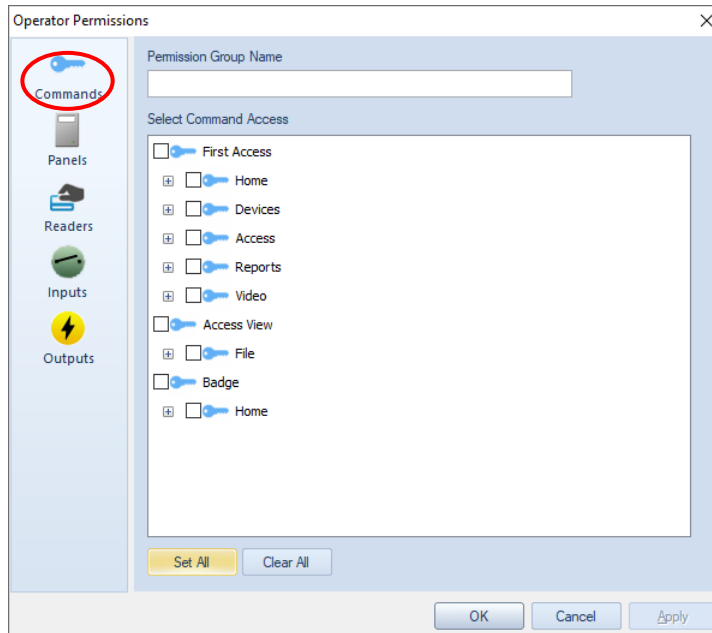


2. Enter a short operator name e.g. Cansec.
3. Enter the password and enter it again on the next line to confirm.
4. Enter the idle time out in minutes to automatically log the operator out of the software. Enter 0 for the software not to log out at all.
5. For **First Access Advanced** only, select an appropriate group to assign to the operator. See *Operator Group Permission* section.

❖ Operator Group Permission

Operator group permissions provide options to create different operator groups with individual permissions for devices and commands. There is a default operator group called **Full Access** which has all permissions assigned.

1. Select  from   to create a new group.

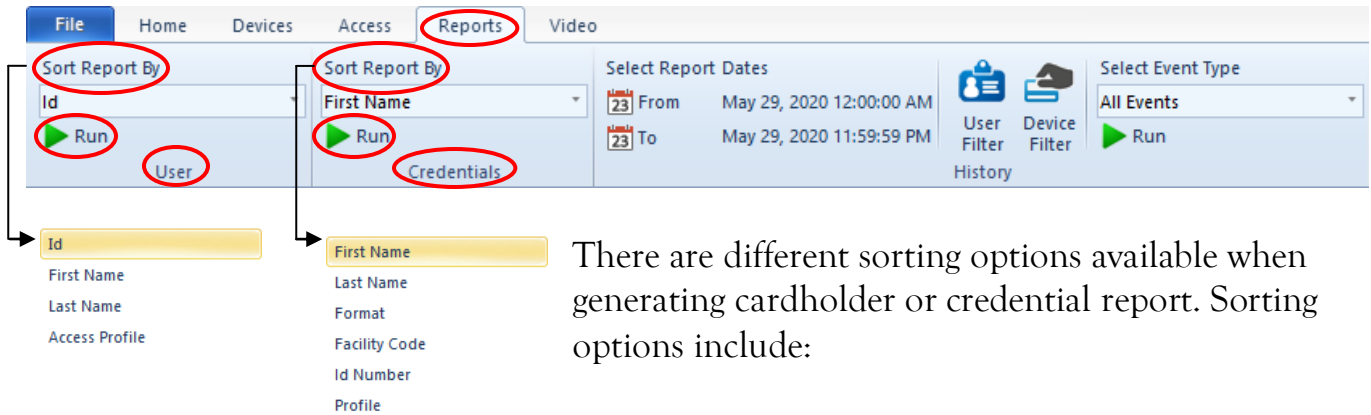


Select commands alone do not allow commands to apply to anything. Devices must also be selected for the commands to be applied to

Video and Badge are add-on software which must be purchased separately. Video deals with NVR integration and Badge deals with photo badge.

2. Enter a name for the group e.g. Restricted or HR or Security Guard etc...
3. Select desired commands and panels, readers, inputs and outputs points that you would like operators to have access to.
4. Click **OK** to save. If necessary, follow the same steps above to create multiple groups with different permissions.
5. To delete a group, select  then select a desired group to delete.
6. To modify permissions for a group select  then select a desired group to modify permissions.

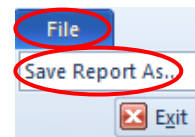
CARDHOLDER AND CREDENTIAL REPORT



There are different sorting options available when generating cardholder or credential report. Sorting options include:

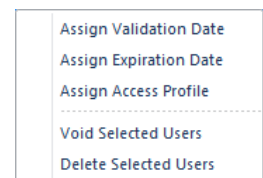
➤ User Report – display all the users

1. Pick the **User** then select a desired sorting option.
2. Click **Run**. Save report in csv format if necessary.



Pin	User Id	First Name	Last Name	Validate	Void	Status	Profile	Field1
00000000	1464285081	Cansec	Support	26-05-16 00:00	01-01-50 00:00	Active	Managers	
00000000	1464285338	John	Doe	26-05-16 00:00	01-01-50 00:00	Active	Accounting	

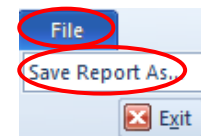
Optionally, select a cardholder or select multiple cardholders and right click to display a pop-up menu from which quick commands can be performed. This can be used to assign multiple cardholders to a common validation date, expiration date or to a common access profile. Multiple cardholders can also be:



- Voided – Credentials' status are set to **Inactive**. Access is not granted at any door. However, the records are kept in the database for the purpose of potential re-activation.
- Deleted – The records are permanently deleted from the database and from the controllers. Access is not granted at any door.

➤ Credential Report – display all the credentials of the users

3. Pick the **Credentials** then select a desired sorting option.
4. Click **Run**. Save report in csv format if necessary



First Name	Last Name	Id Format	Facility Code	Id Number	Profile
Augustine	Duford	Cansec 37 Bit	2864	01437	Lockers
Augustine	Duford	Cansec 37 Bit	2864	01691	Front Door
Aura	Delacote	Cansec 37 Bit	2864	00188	Front Door & Garage
Bader	Frères	Cansec 37 Bit	2864	00128	Laundry
Belma	Grace	Cansec 37 Bit	2864	00838	Front Door & Garage

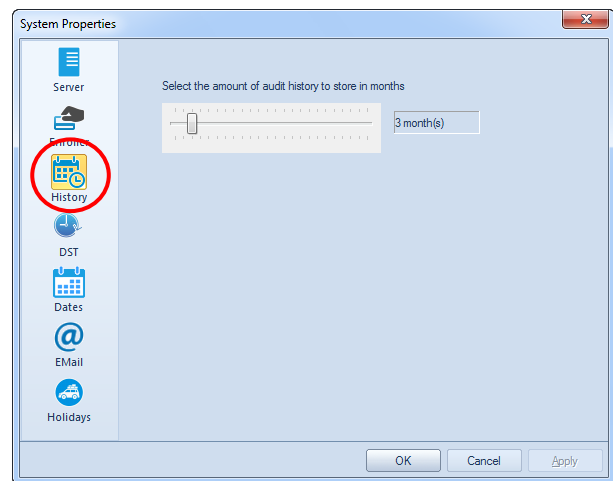
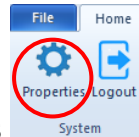
Step 5. History and Audit Report

HISTORY RETENTION

The First Access software records all events on the computer's hard drive. Because **First Access** is a “real-time” system, these events are constantly being recorded in the Microsoft SQL Database. To specify the retention period, perform the following steps:

1. Launch System Properties
2. Select **History** tab.
3. Use the slider to specify retention period in a month. Click **OK** when done.

Note: *Once a month the system will scan and discard any history entry older than the specified month.*



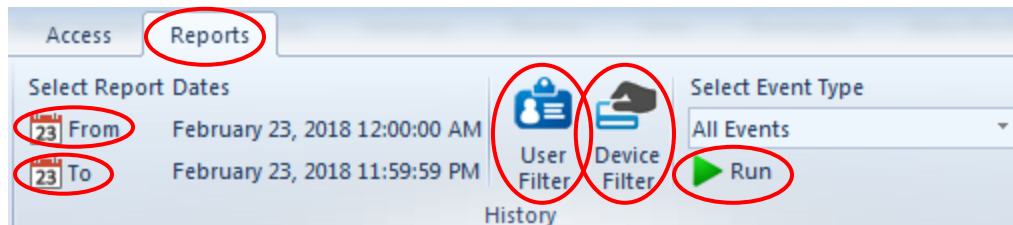
ON-BOARD AUDIT EVENT STORAGE

The MAP control panel is capable of storing a maximum of 10,000 events in its memory when the panel does not communicate with the software. When 10,000 events have been reached, new events will replace the oldest events. When the panel resumes its communication, all old and new events are sent to the computer in real time freeing its memory for storage when the communication is not established and panel goes offline. The panel must have a backup battery to prevent all historical events from being lost from its volatile memory storage when a power outage occurs. All other settings are saved in non-volatile memory storage.

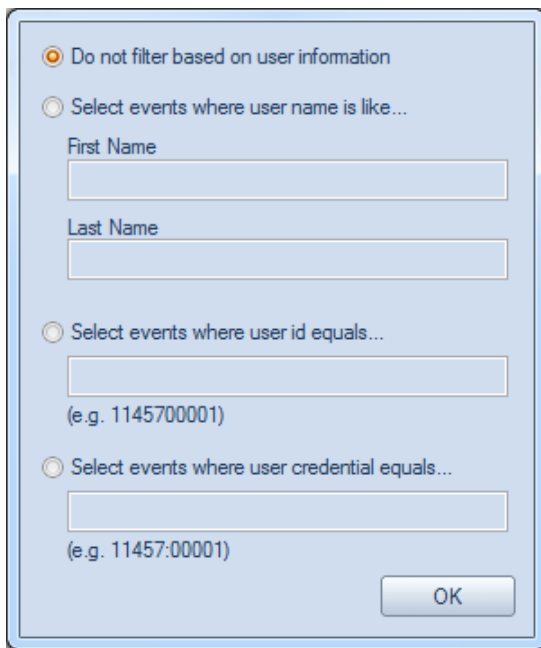
VIEW AUDIT HISTORY

To view all audit history events stored in the database:

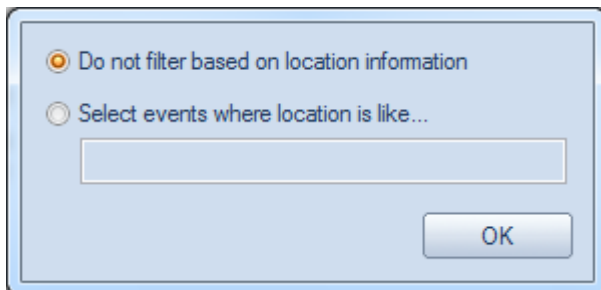
1. Select **Report** from the top main menu.



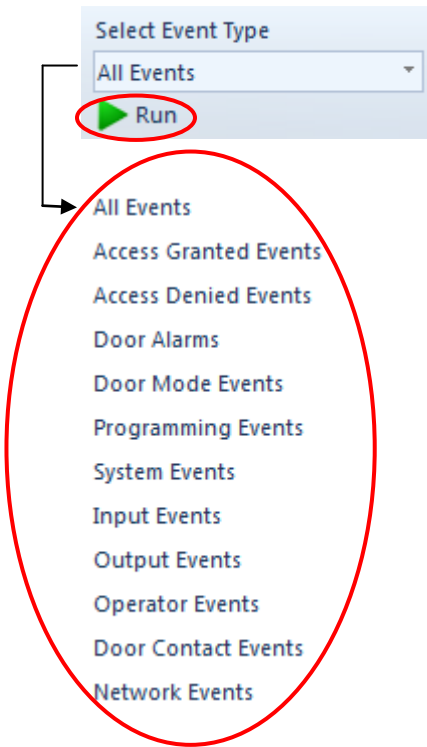
2. Select Month, Day and Year for **From** date.
3. Select Month, Day and Year for **To** date.
4. Optionally select **User Filter** to generate a report for a particular user.



5. Optionally select **Device Filter** and enter device name e.g. *Front Door* to generate report for that door only.



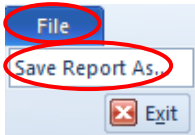
6. Select a filter for the **Event Type**.



7. Click the **Run** button. 

Events Audit Query								
Date	Time	Event	Name	Id	BitCount	Credential	Operator	Location
02-11-17	09:43:18	Operator Login	admin					CANSEC-PC09
02-11-17	09:43:18	Access Granted Unlock, Schedule 1	Nguyen, Minh	1507040401	37	20063:07460	Reader	IT Room
02-11-17	09:43:20	Card Reader Relocked	Nguyen, Minh	1507040401	37	20063:07460	Reader	IT Room
03-11-17	00:00:00	System Clock Time Set					FA Server	First Panel
03-11-17	08:00:00	Card Reader Unlocked					Schedule	IT Room
03-11-17	16:15:00	Card Reader Relocked					Schedule	IT Room

8. Save report in csv format if necessary.

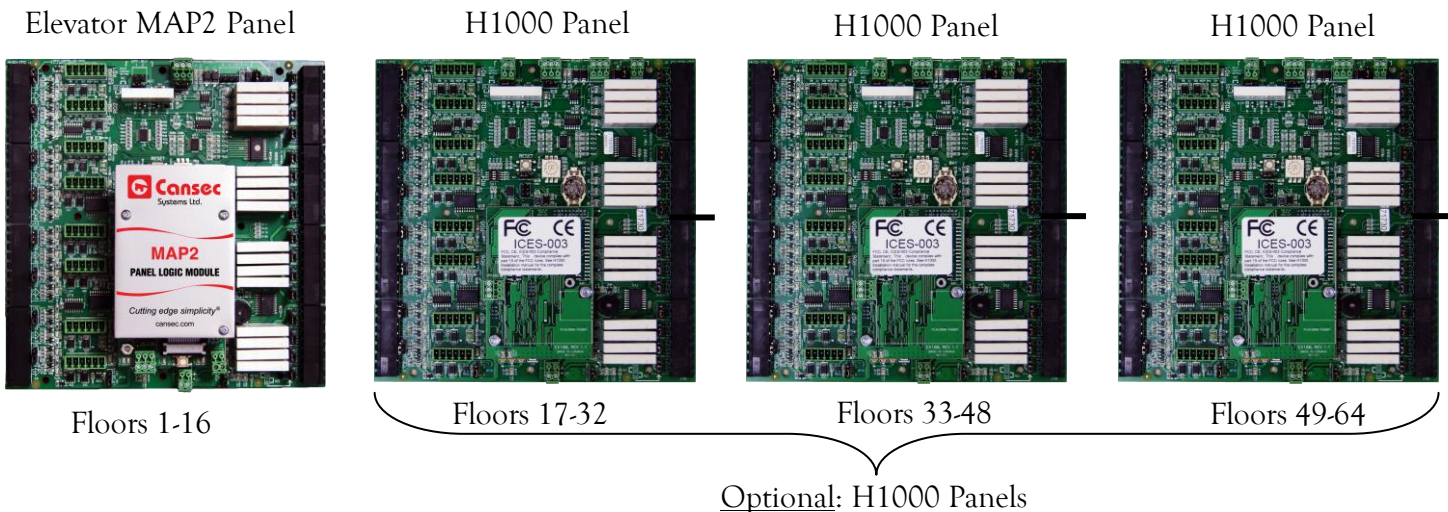


Elevator

The **First Access** software, both Express and Advanced versions, supports MAP2 panel provisioned for elevator mode. The MAPmini and MAP1 panel does not support elevator mode.

The elevator MAP2 panel alone supports up to 16 floors. However, with the optional add-on dedicated H1000 panels, the MAP2 panel supports up to a maximum of 64 floors.

Elevator MAP2 Panel must be provisioned by Cansec each time an additional add-on H1000 panel is added

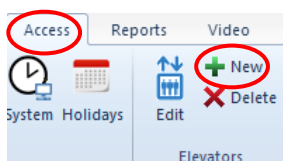


FLOOR GROUPS, ACCESS GROUPS AND FLOOR-UNLOCK SCHEDULE

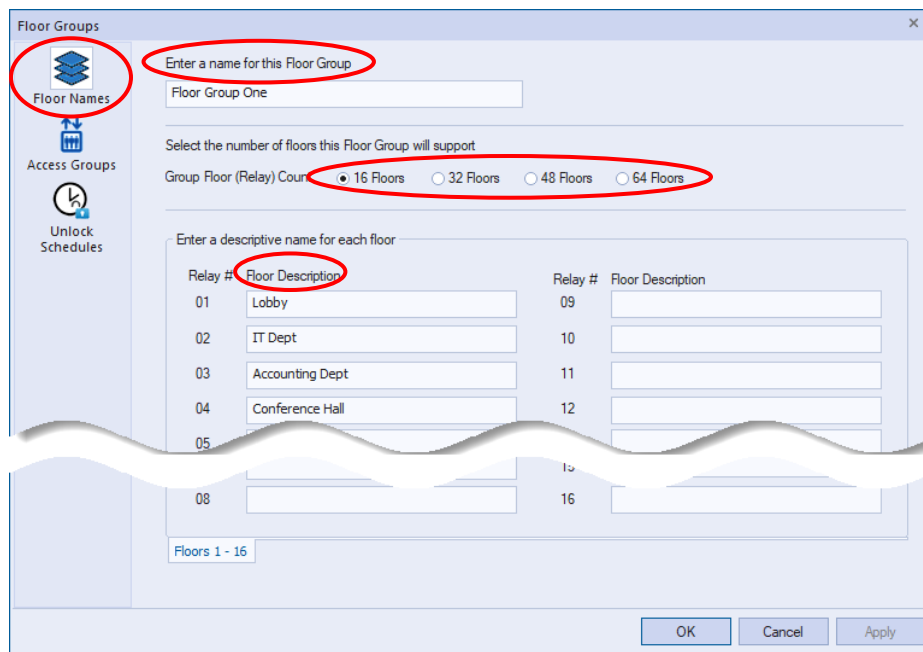
The elevator floor group defines a set of floors that an elevator handles. The access group defines who may access those floors. The optional floor-unlock schedule defines when selected floors may be freely accessible to everyone.

Typically, there is just one floor group and one elevator, but there are cases where multiple elevators are used to serve different floor sets e.g. elevator one serves floors 1 to 32 while elevator two serves floors 33 to 64.

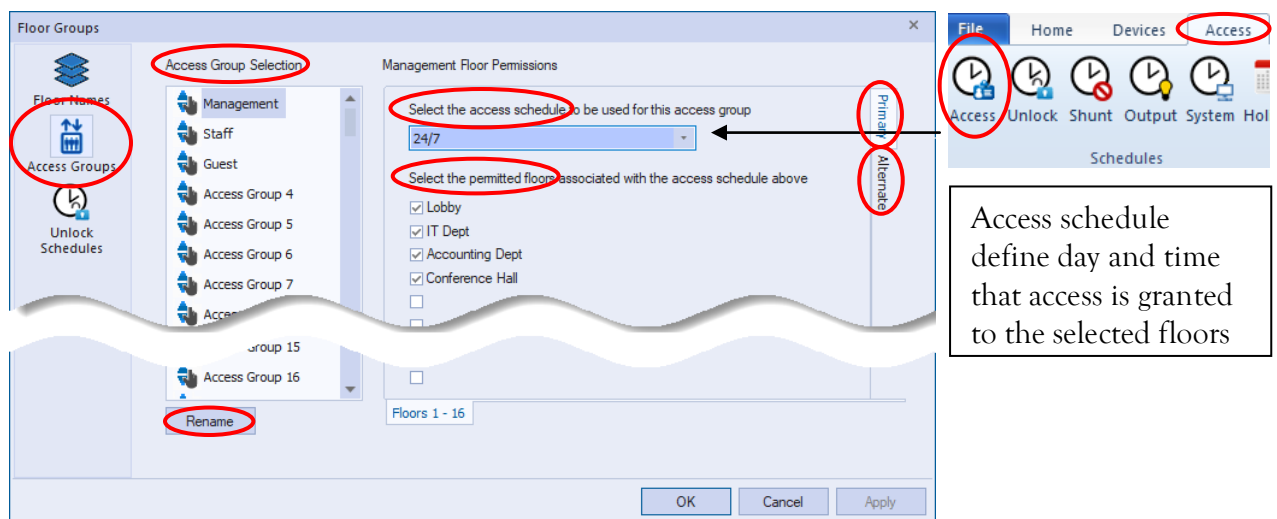
1. If not already created then create a new elevator floor group from the top menu **Access** under the **Elevators** sections



2. Enter a name for the floor group e.g. *Floor Group One*



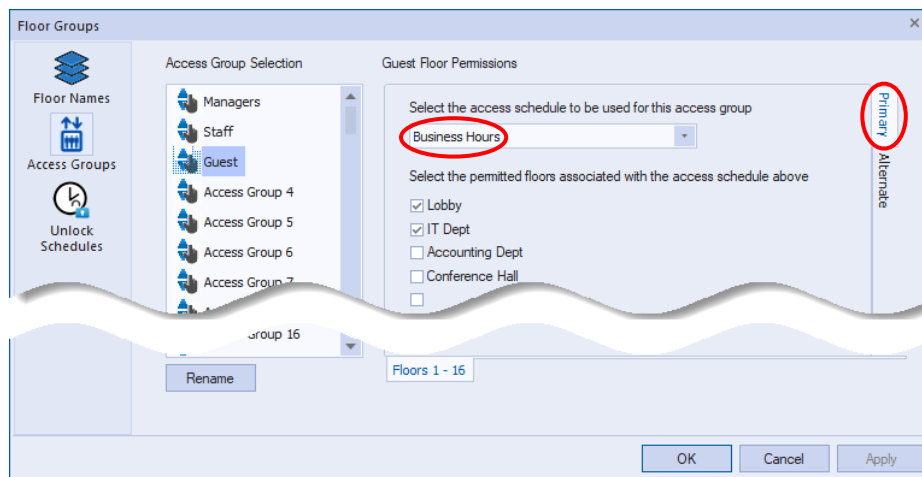
3. Select the desired number of floors (16, 32, 48 or 64) that this elevator group will support and name each floor accordingly.
4. Select an **Access Group** then select a desired primary and optional alternate access schedule and floors that this access group is permitted to access. Rename the group as desired e.g. *Management*, *IT Department*, *Guest* etc...



➤ Primary Schedule

Primary schedule is used to specify floors that are permitted during certain days and times.

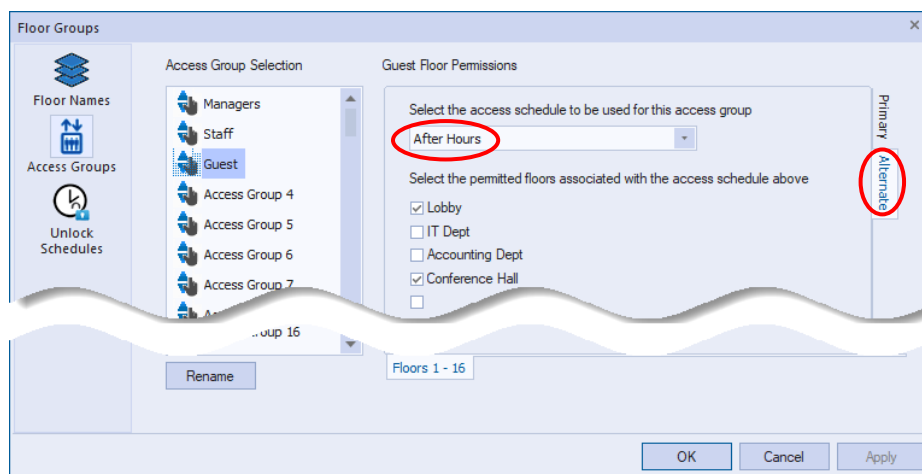
This example shows that the Guest group has access only to Lobby floor and IT Dept floor during business hours.



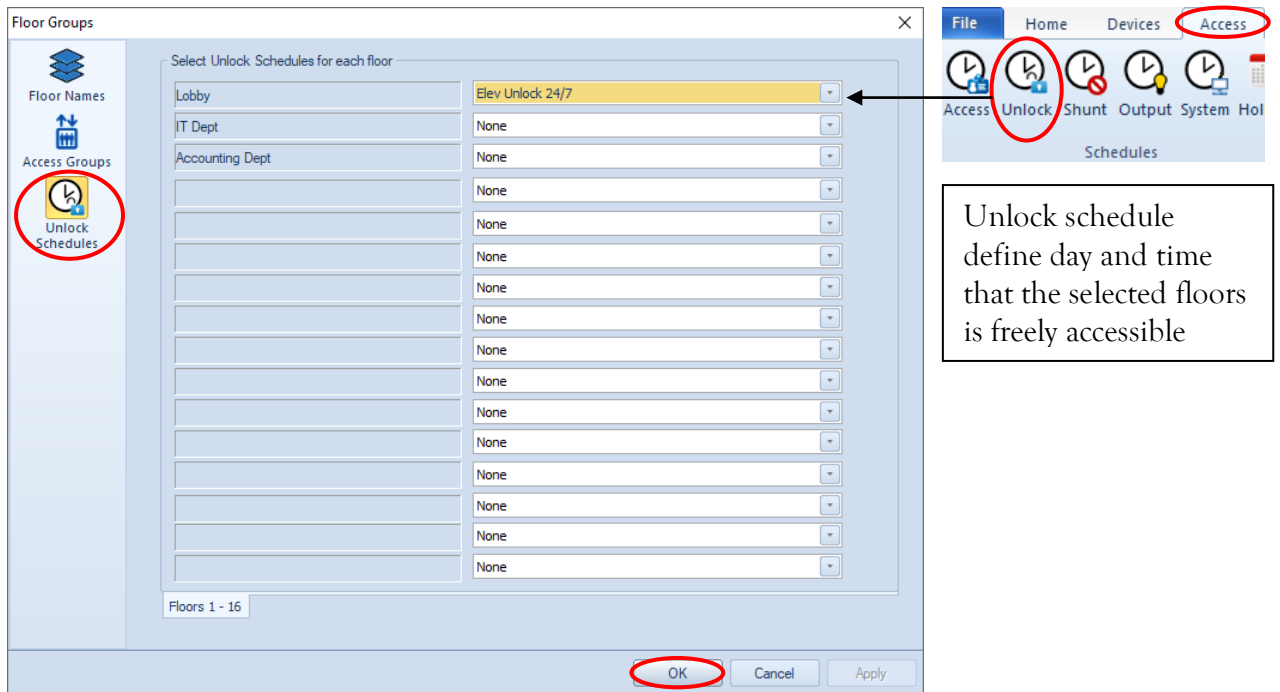
➤ Alternate Schedule

Alternate schedule is used to specify floors that are permitted outside of the primary schedule.

Continuing with the above example, we can now use the alternate schedule to select only Lobby and Conference Hall floors are permitted for the Guest group after hours.



5. If a floor is required to unlock for the purpose of free access then select **Unlock Schedules**. Next, select a desired floor and choose an unlock schedule to assign to it. If necessary, repeat similar steps for other floors.

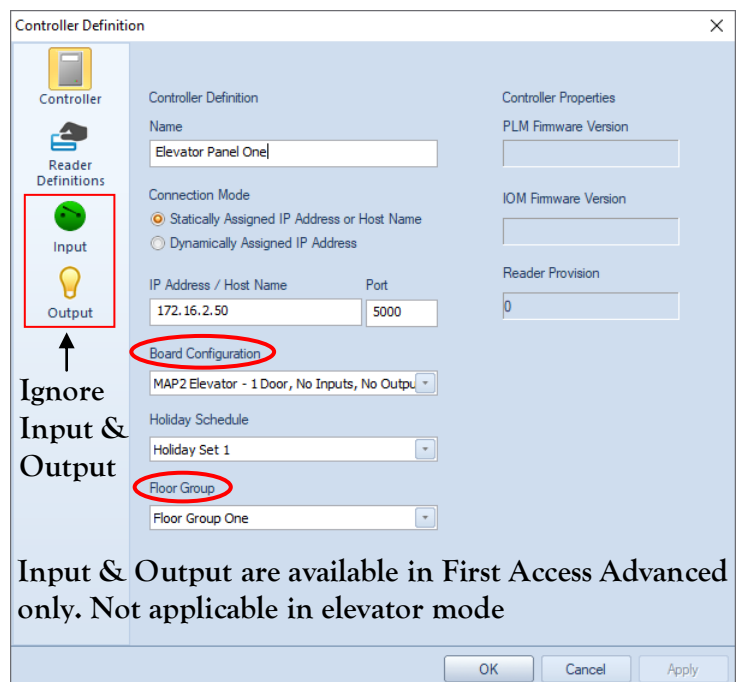


ADD ELEVATOR PANEL

1. Select **Devices** -> **Managed** -> **New** from the top menu



2. Name the panel e.g. *Elevator Panel One* etc...
3. Select appropriate connection mode.
4. Select *MAP2 Elevator* for board configuration and assign it a floor group that it will handle.



Input & Output are available in First Access Advanced only. Not applicable in elevator mode

5. Enter a name for the reader e.g. *Main Elevator*. Ignore options that are related to doors e.g. Multi-Function Relay, DHO duration etc... Click **OK** when done.

Controller Definition

Select Reader Definition from the Drop List Below

Reader1

Id: 9, Name: Main Elevator

Unlock Duration: 7, Multi-Function Relay: Not Used

DHO Duration: 60, Reader / Key Pad Mode: Card Only

Pre-Alert Duration: 30, Facility Code for Keypad Card Id (0 - 255): 0

System Schedule for PIN Bypass: None

Unlock Schedule: None

CCTV / DVR Camera: None

RTE Polarity: NO to NC, NC to NO

Double Bump: Unlock / Relock, Use as Trigger

Advanced Options, Defaults

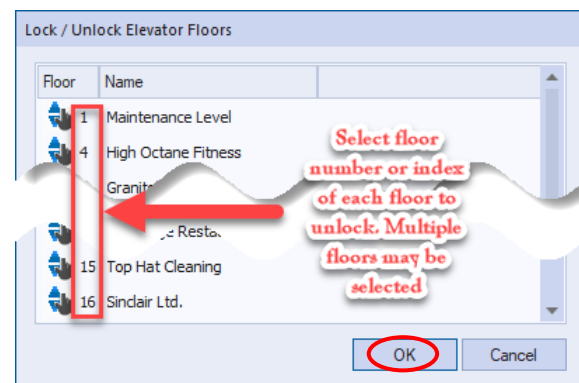
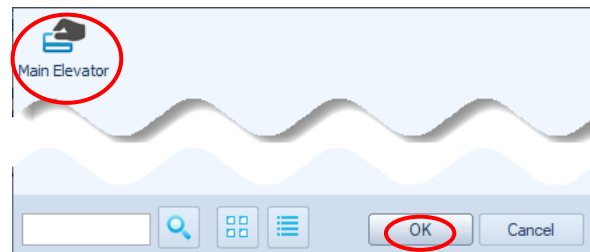
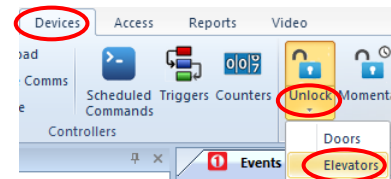
OK, Cancel, Apply

Ignore these options

MANAGE ELEVATOR FLOORS

➤ Floor Unlock

1. Select **Devices** and select the down arrow of the **Unlock** button then select **Elevators**. Select a desired elevator.
2. Select floors to be unlocked.
3. Click **OK** when done.

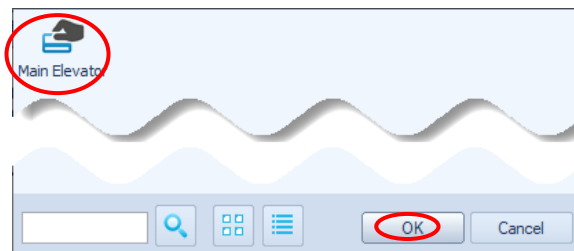


➤ Floor Relock

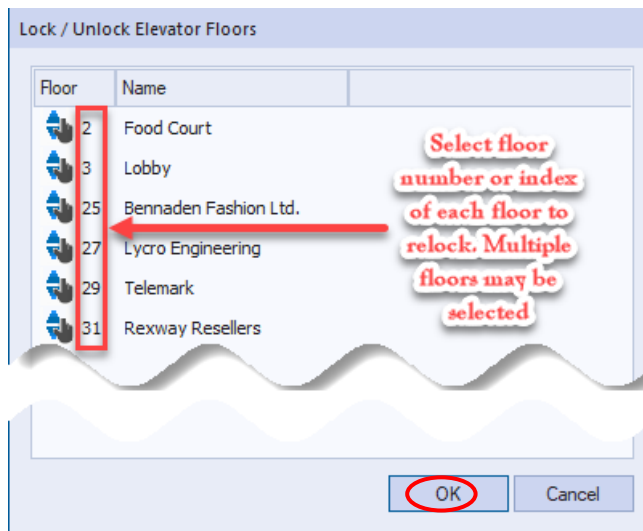
1. Select **Devices** and select the down arrow of the **Relock** button then select **Elevators**.



2. Select a desired elevator.



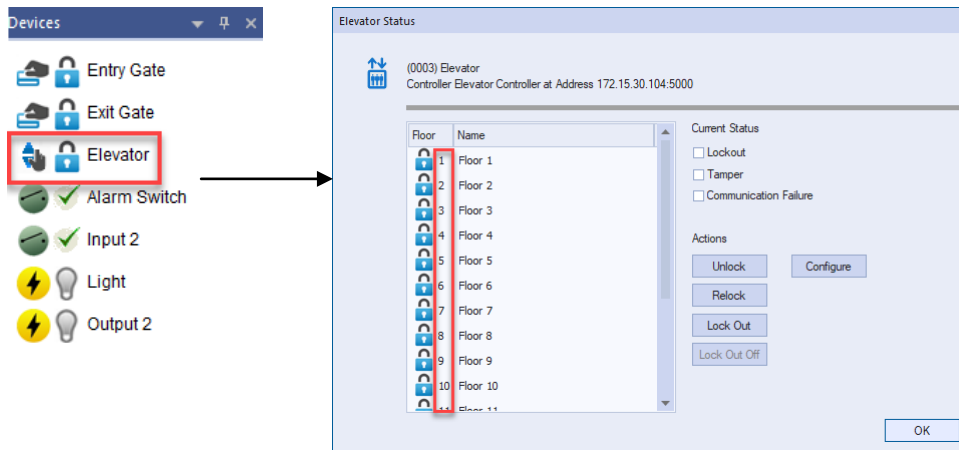
3. Select currently unlocked floors to relock them.



4. Click **OK** when done.

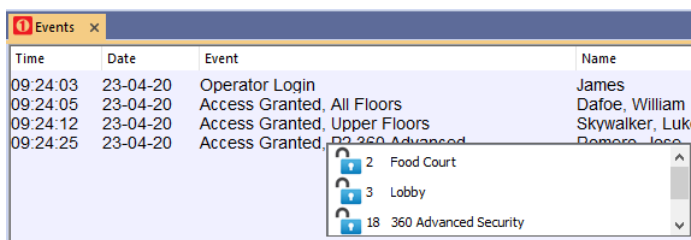
➤ Floor Unlock & Relock

Alternatively, select the elevator in the device view to launch the Elevator Status screen. Select desired floors using the floor number and unlock or relock accordingly. Single or multiple floors may be selected.



➤ Access Granted Event

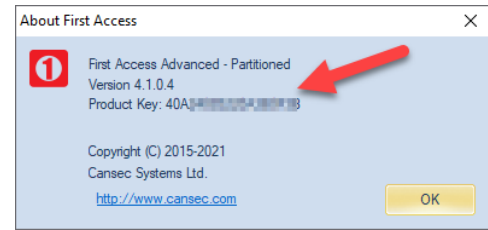
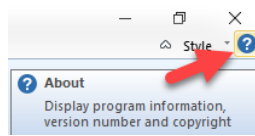
When an access-granted event for the elevator is displayed in the **First Access** software, click on that event to display the pop-up box which shows the floors that were unlocked. Click on the pop-up box to dismiss it.



Software Update & Upgrade

➤ Software Update: Old version to new version

- If you have First Access Advanced then select the question mark (?) on the top right corner of the software to display the version and the software/product key information. Record your software key.



- Back up the database as a precaution. See *Appendix section for instructions to back up the database*. Remove the old version through add/remove program. The database will not be removed during the software removal.

Apps & features

Optional features

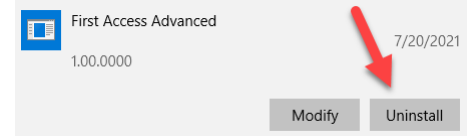
App execution aliases

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

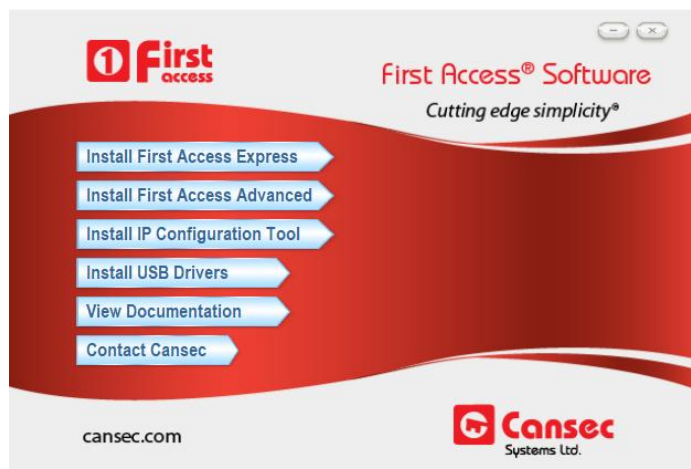
first

Sort by: Name Filter by: All drives

1 app found



- Download the latest version of the First Access software from <https://www.cansec.com/downloads.html>. Unzip and launch the installation package. If you have First Access Express then select Install First Access Express and otherwise select Install First Access Advanced which requires a software key you have recorded previously. During the installation the software will automatically update the database accordingly.



If you have workstations with First Access clients installed then they must be removed and reinstalled with the latest version

➤ Software Upgrade: First Access Express to First Access Advanced

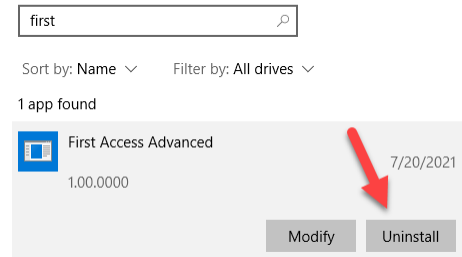
- Purchase the software key from your dealer then download the latest version of First Access software from <https://www.cansec.com/downloads.html>.
- Back up the database as a precaution. See *Appendix section for instructions to back up the database*. Remove the old version through add/remove program. The database will not be removed during the software removal.
- Unzip and launch the software installation package you have downloaded.

Apps & features

Optional features

App execution aliases

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.



If you have workstations with First Access clients installed then they must be removed and reinstalled with the latest version

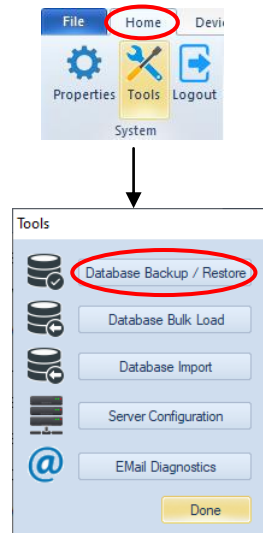
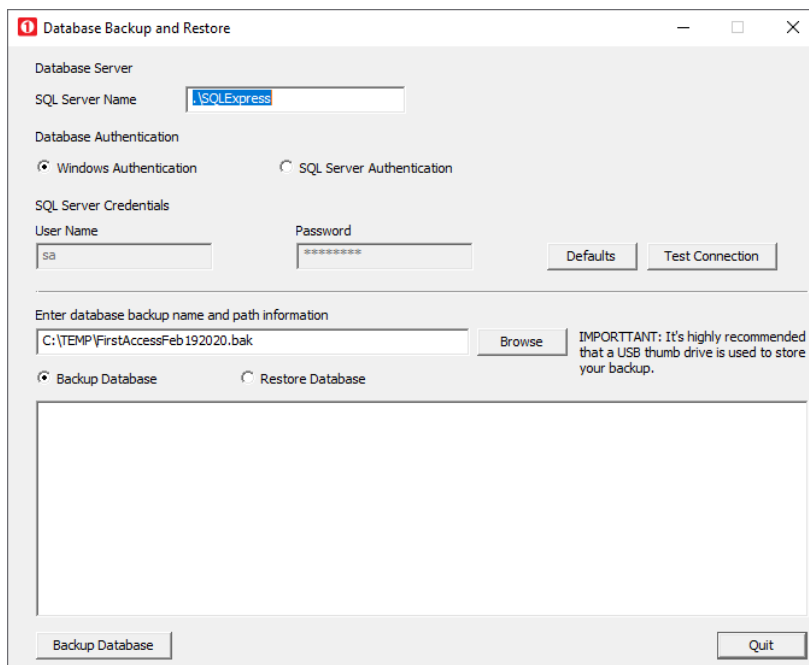
- Select Install First Access Advanced then supply the software key when prompted. During the installation the software will automatically update the database accordingly.

Appendix

DATABASE BACKUP & RESTORE UTILITY

The **Database Backup and Restore Utility** provides options to back up the database or to restore the database from a backup. The utility is only applicable for the Microsoft SQL database that was installed by **First Access** software. It's required that the backup be done regularly and preferably by an IT personnel or database administrator and stored offsite for recovery when needed.

1. Launch Database Backup/Restore from the Tools menu.
2. The server name and SQL instance is normally `.\SQLExpress` but if you have used other instance name like `.\SQLFA` then enter the appropriate name.
3. Select either Windows or SQL Server Authentication.

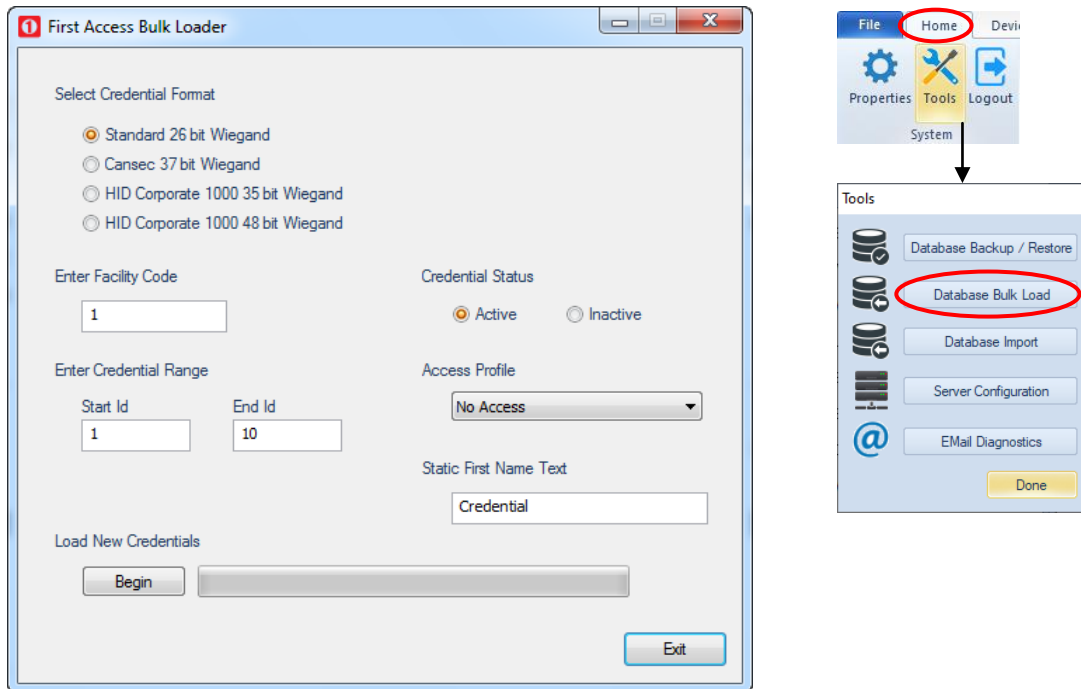


4. To backup the database, select **Backup Database** option and click **Browse** to select the location to save the backup file to. Click **Backup Database** button
5. To restore the database, select **Restore Database** option and click **Browse** to select the location where the backup file was saved to. Select the back file and click **Restore Database** button.
6. Select **Quit** when done.

BULK CREDENTIAL LOAD UTILITY

The **Bulk Credential Load Utility** provides an option to load several credentials of certain format without the need to load one credential at a time.

1. Launch **Database Bulk Load** from the Tools menu.

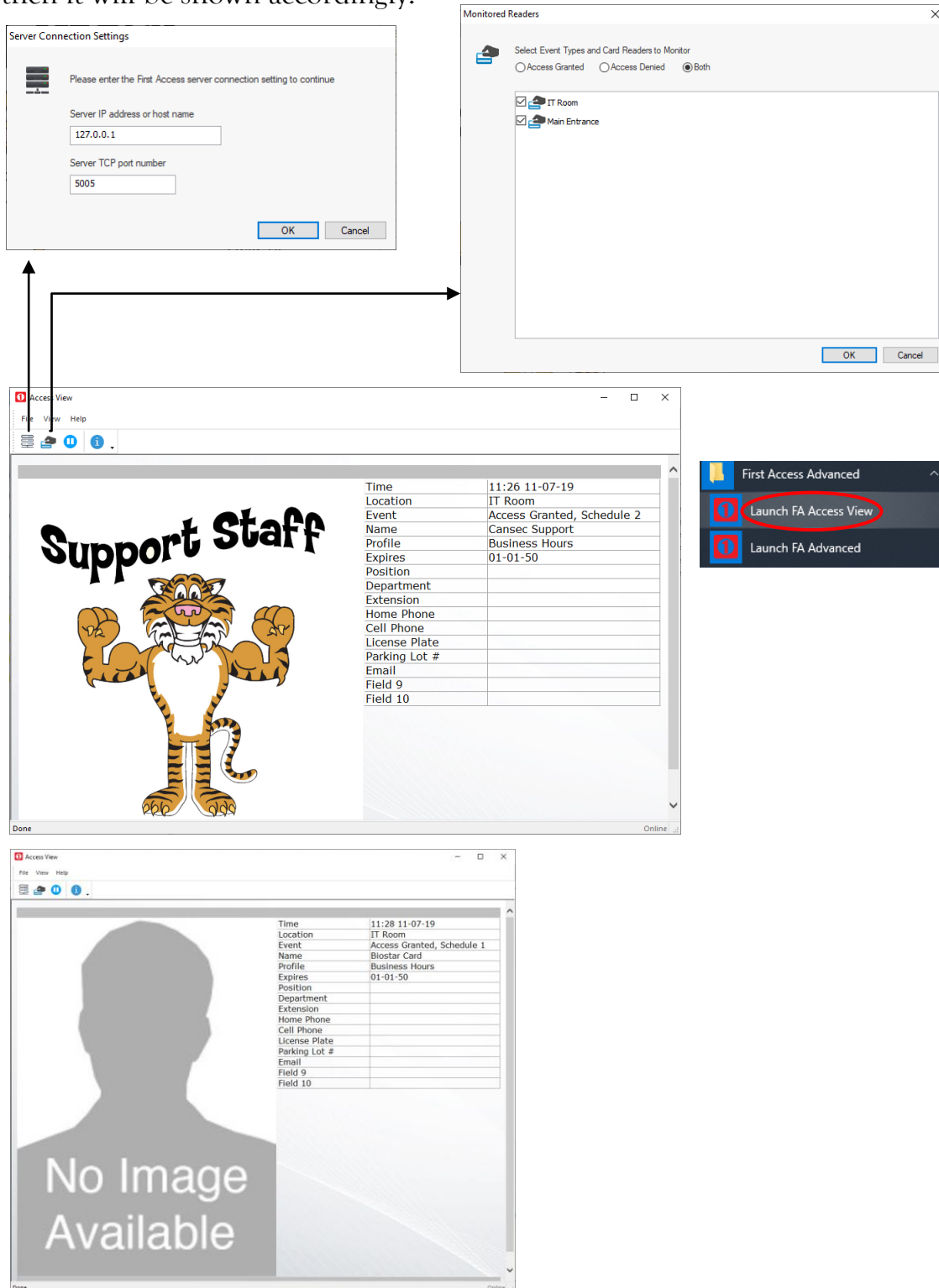


Note: The information about your credential e.g. format, system/facility code and credential range are usually printed on the box. If unsure, contact your dealer or the place where you have purchased your credential from.

2. Select the format of your credentials and enter the **Start Id** and **End Id**. Select the status either Active, for the credentials to be active immediately, or Inactive which can later be set to Active. Select a desired Access Profile and enter a generic name for all credentials. The name can later be modified to the actual name of the credential owner before or as credentials are handed out to the owner.
3. Select **Begin** to load all credentials.
4. Follow the prompt to download to the panels  **Download**
5. If more than one types or formats of credentials are available then repeat the same steps to load them. Otherwise select **Exit**.



The **FA Access View** utility provides an option to view access events of cardholders from selected readers. The event can either be access granted event or access denied event or both events. If the cardholder has an image imported to his/her record then it will be shown accordingly.

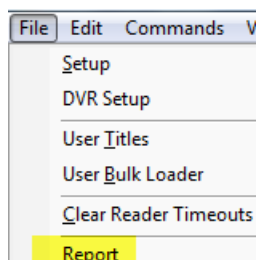


FIRST ACCESS IMPORT UTILITY

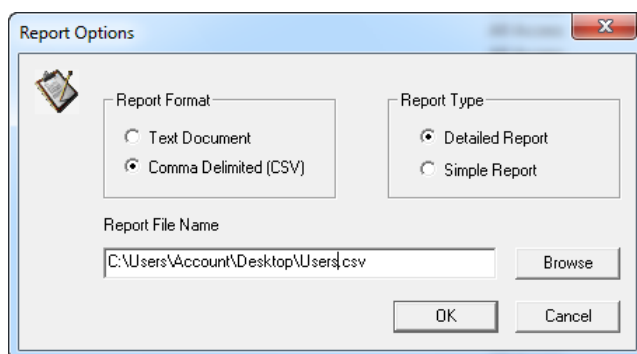
The Import Utility provides an option to import the user database, exported to a csv file from either SmartLock Pro, SmartLock Pro Plus or Hurricane software, into the First Access database.

- Export from SmartLock Pro or SmartLock Pro Plus

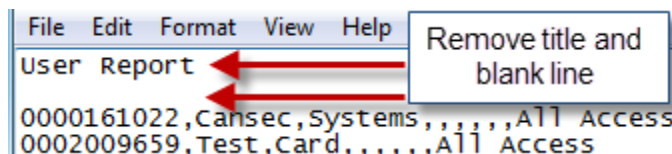
1. Select  (Pro Plus) or  (Pro) from the left panel.
2. To top left menu, select File->Report



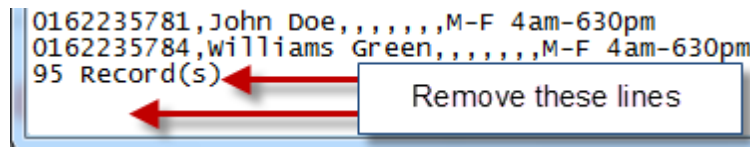
3. Select “Comma Delimited (CSV)” and select “Detailed Report”



4. Click **Browse** to select a location to save the csv report file to. Enter a name for the file e.g. *ProPlusUsers.csv*
5. Click **OK** when done.
6. Use **Notepad** (*Do not use Excel application because it removes leading zeros from card number*). Open the file and remove the title and any blank line.



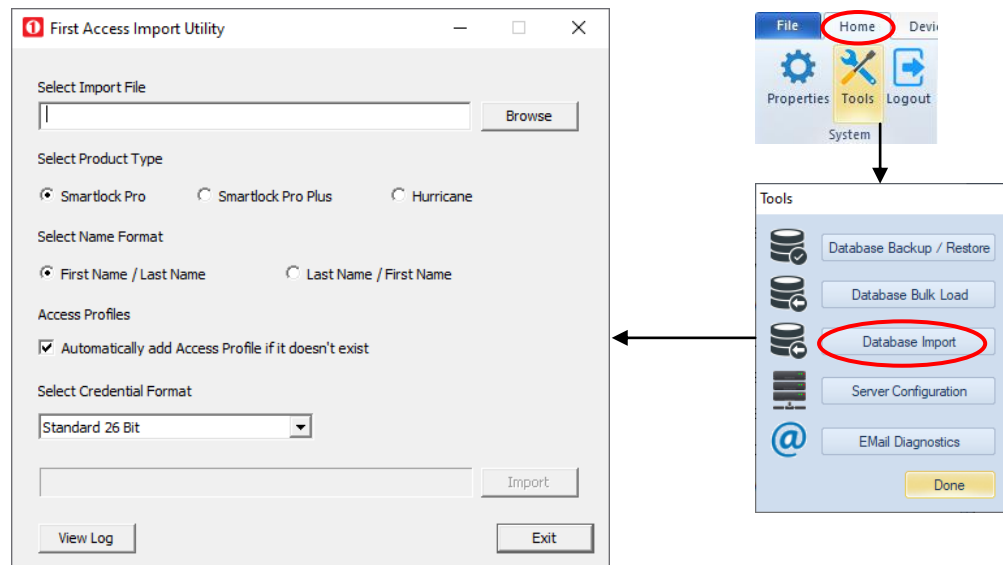
- At the end of the file, remove the record counter and any blank line.



- Save the file to get it ready for import.

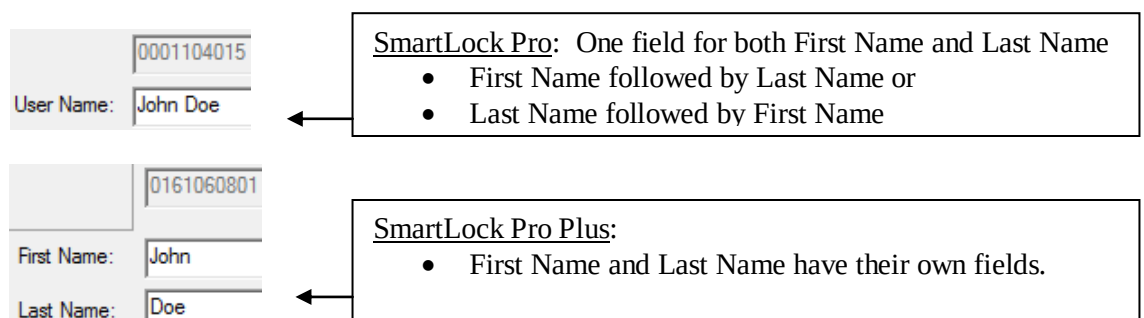
- Import to First Access**

- Launch **Database Import** from the Tools menu once the csv file has been exported from either Pro or Pro Plus.
- Click **Browse** to locate and select the exported csv file.



- Select the product type e.g. *SmartLock Pro* or *SmartLock Pro Plus* that the csv file was exported from.

Note: The Name Format selection is applicable to *SmartLock Pro* only since *Pro* has only one field for both First Name and Last Name.

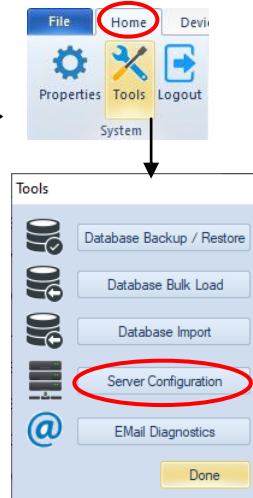


4. For SmartLock Pro, select if the **User Name** field contains First Name followed by Last Name or Last Name followed by First Name. This way, the names will be imported accordingly into First Access.
5. Select the credential format that the users have. Usually, all users carry the same credential format. If users carry different formats then the csv file must be edited to group users having the same format together, save them in different csv files and import one file at a time.
6. Click **Import** to import the exported csv file.
7. Click **View Log** to review any error message that may have happened during the import.
8. Click **Exit** when done.

SQL SERVER CONNECTION CONFIGURATION UTILITY

The **Server Configuration Utility** provides an option to configure or modify the SQL server connection information.

1. Launch **Server Configuration** from the Tools menu.



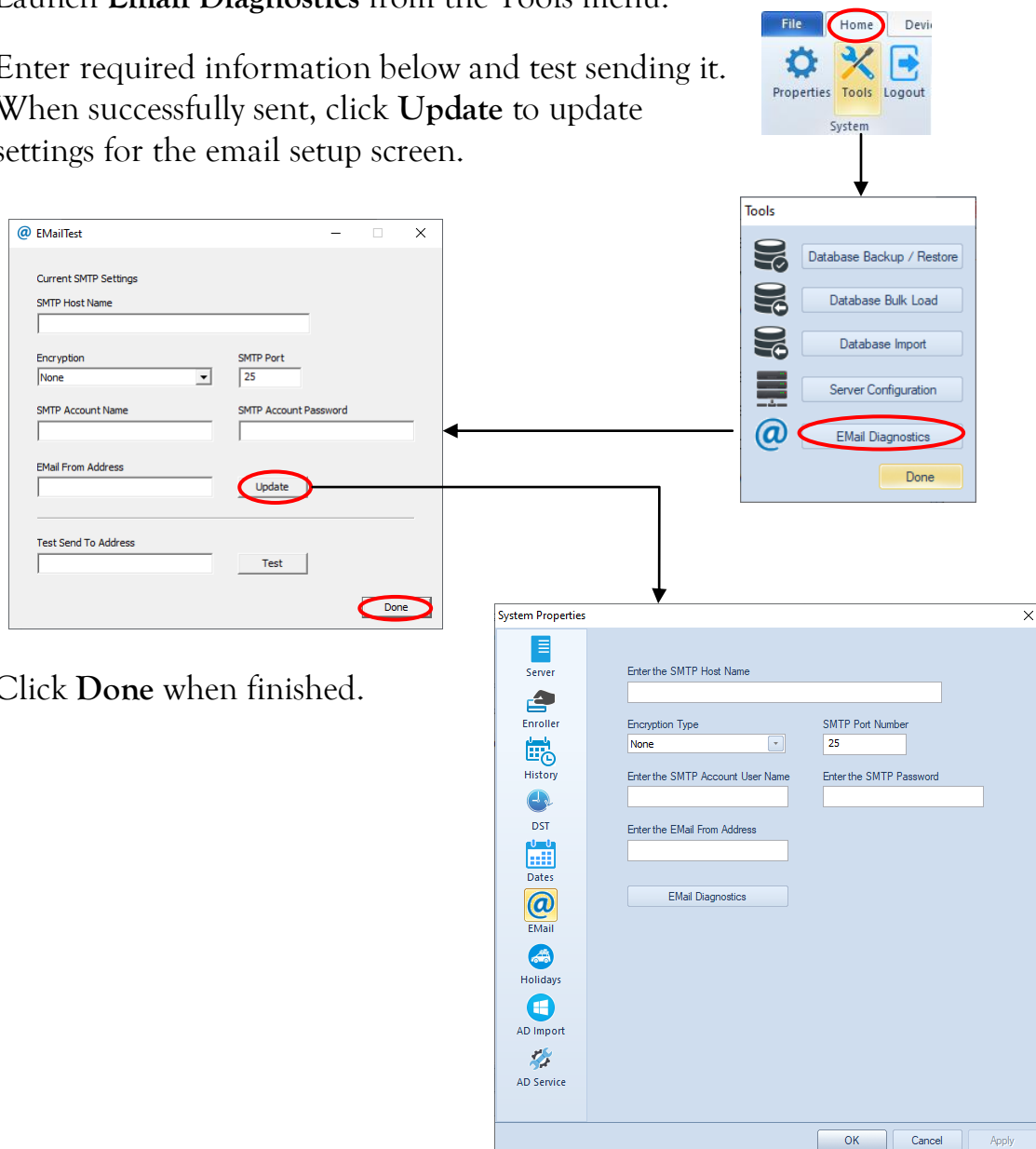
The configuration should be done by IT personnel or by database administrator. The default configurations are configured during the software installation. These steps should be performed only when there is a change to the server e.g. a migration of the server.

2. Enter the SQL server name along with its instance if necessary.
3. Select appropriate authentication method, build the string connection and click **Test** to test the connection.
4. Click **Save** to save the configuration if the connection is successful.
5. Click **Exit** when done.

EMAIL DIAGNOSTICS

The **Email Diagnostic** tool is available in **First Access Advanced** only. The tool provides an option to configure and diagnose email setup.

1. Launch **Email Diagnostics** from the Tools menu.
2. Enter required information below and test sending it. When successfully sent, click **Update** to update settings for the email setup screen.



3. Click **Done** when finished.

DAILY SYNCHRONIZATION

➤ Clock Synchronization

Every day at 3:00 AM the **First Access** server software would automatically synchronize the clock from the computer to all the panels. Since the computer has the built-in Daylight Saving Time (DST) feature so this would take care of the DST for all the panels.

03:00:00	01-01-19	System Clock Time Set	FA Server	Main Panel
03:00:00	02-01-19	System Clock Time Set	FA Server	Main Panel

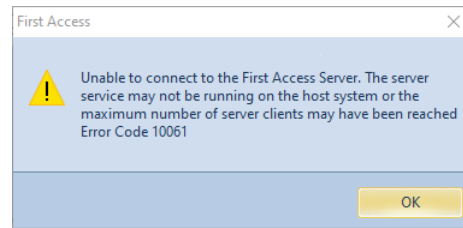
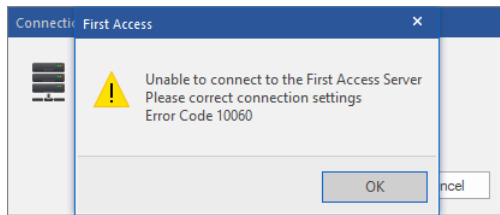
➤ Data Synchronization

Every day at 1:00 AM the **First Access** server software automatically synchronizes data only to those panels that are flagged as unsynchronized. For example, changes were made to the database like adding new users but some panels are offline. Those offline panels will be flagged as unsynchronized and will be synchronized at 1:00 AM. However, if those panels are online before 1:00 AM and the operator does a manual download to those panels then they are not flagged as unsynchronized.

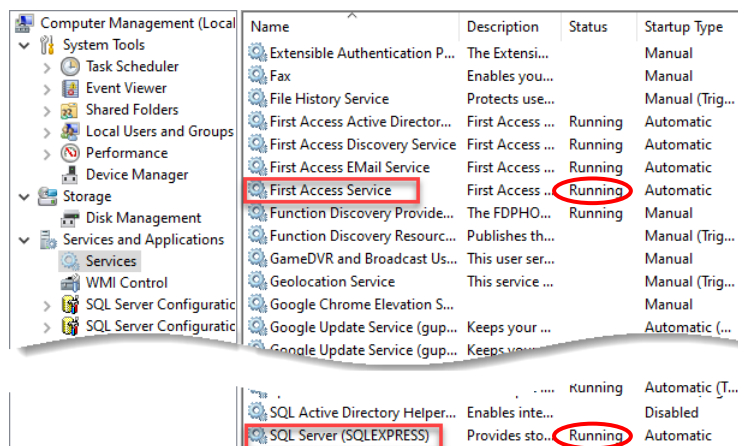
Date	Time	Event	Name	BitCount	Credential	Operator	Location
11-01-20	01:00:01	System Clock Time Set				Sync Task	Sim Unit 1 (P3)
11-01-20	01:00:01	System Clock Time Set				Sync Task	Sim Unit 3 (HO)
11-01-20	01:00:01	Reader Configuration Updated				Sync Task	Sim Unit 3 - Reader 1 (HO)
11-01-20	01:00:01	System Clock Time Set				Sync Task	Sim Unit 2 (P3)
11-01-20	01:00:01	Reader Configuration Updated				Sync Task	Sim Unit 1 - Reader 1 (P3)
11-01-20	01:00:01	Reader Configuration Updated				Sync Task	Sim Unit 2 - Reader 1 (P3)
11-01-20	01:00:01	Unlock Schedule 0 Updated				Sync Task	Sim Unit 3 (HO)
11-01-20	01:00:01	Unlock Schedule 0 Updated				Sync Task	Sim Unit 1 (P3)
11-01-20	01:00:02	Unlock Schedule 0 Updated				Sync Task	Sim Unit 2 (P3)
11-01-20	01:00:02	Reader Configuration Updated				Sync Task	Sim Unit 3 - Reader 1 (P3)
11-01-20	01:00:03	Access Schedules 11 to 15 Updated				Sync Task	Sim Unit 2 (P3)
11-01-20	01:00:03	Output Schedule 0 Updated				Sync Task	Sim Unit 1 (P3)
11-01-20	01:00:03	Access Schedules 16 to 20 Updated				Sync Task	Sim Unit 3 (HO)
11-01-20	01:00:03	Output Schedule 0 Updated				Sync Task	Sim Unit 1 (P3)
11-01-20	01:00:03	Access Schedules 16 to 20 Updated				Sync Task	Sim Unit 2 (P3)
11-01-20	01:00:03	Access Schedules 21 to 25 Updated				Sync Task	Sim Unit 3 (HO)
11-01-20	01:00:04	Access Schedules 21 to 25 Updated				Sync Task	Sim Unit 2 (P3)
11-01-20	01:00:04	Output Schedule 0 Updated				Sync Task	Sim Unit 1 (P3)
11-01-20	01:00:04	Access Schedules 26 to 30 Updated				Sync Task	Sim Unit 3 (HO)

Troubleshooting

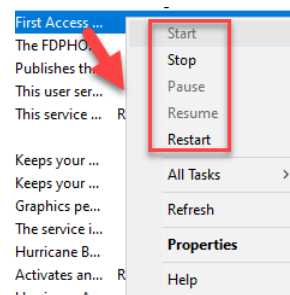
- Unable to connect to the First Access Server when launching First Access Client



- Ensure that the First Access service & SQL Express service are running

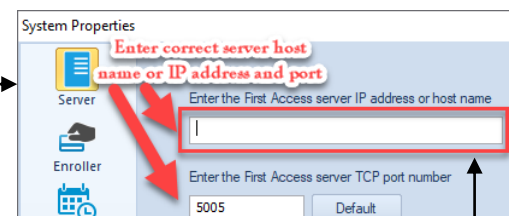


Right click on the service e.g. First Access Service or SQL Server to access the pop-up menu in order to start, stop the service etc...



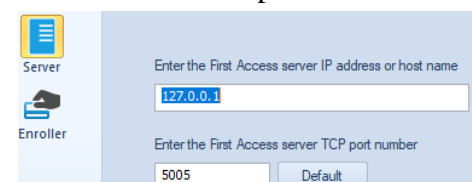
- Ensure that you have not reached the maximum number of clients connecting to the server. First Access Express supports 4 concurrent connections. First Access Advanced supports 20 concurrent connections.

- If the First Access Server is installed on a different computer than the First Access Client then ensure that the IT personnel configure the firewall rule on the server to allow incoming TCP traffic on port 5005 from the clients, and that the host name or IP address of the server is correctly entered in the First Access Clients.

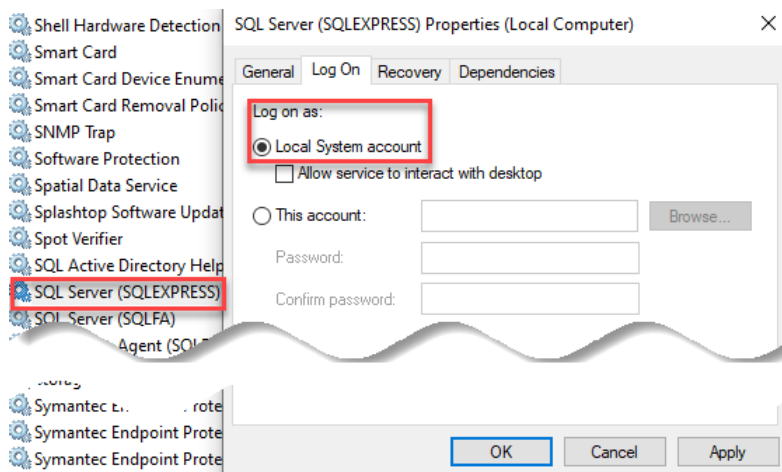


Host name or IP address of the server not 127.0.0.1

- If the First Access Server and Client are installed on the same computer then ensure that the host name or IP address (127.0.0.1) and port (5005) are correct.



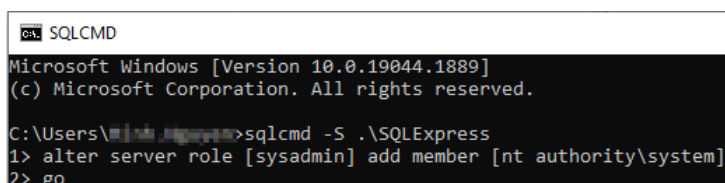
- It's highly suggested to have Cansec software installer to install both SQL and First Access software. During the installation, the installer will inject SQL login credentials with proper privilege in order for the First Access service to connect to create and manage the database. The First Access service will fail to start if it does not have proper login credential. See the log files *C:\ProgramData\Cansec\First Access\Logs\FAService.log* for more details.



- If you manually install SQL or use your own instance of SQL then there are two options:

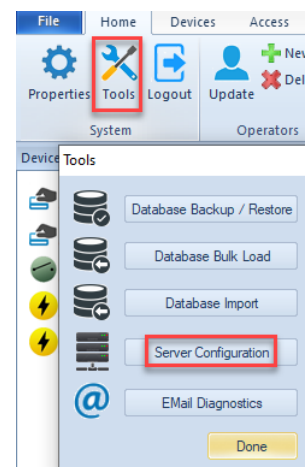
1. Use “Trusted Connection”

Launch the Command Prompt and enter each line, one at a time seen in the image below. Hit enter after each line. If it fails, fall back to option 2.



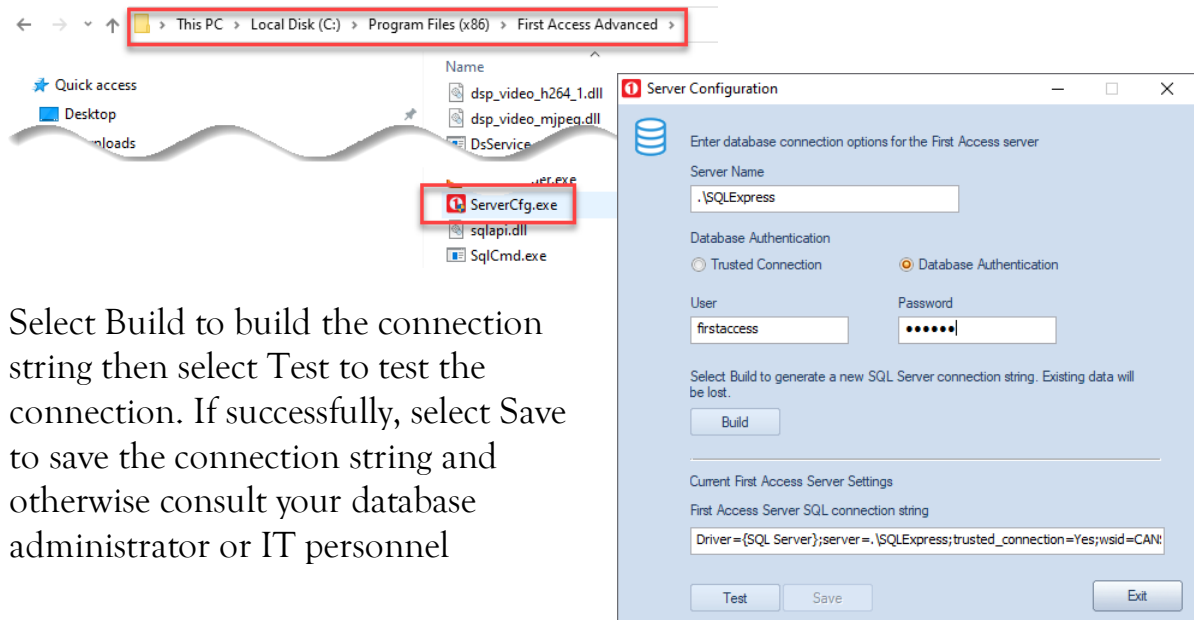
2. Use “Database Authentication”.

Launch First Access client (must be running on the same First Access server) and from the Home menu, select Tool>Server Configuration. Enter the user name and password that you have previously configured when you manually installed SQL. The account must have appropriate privilege to create and manage the database



or otherwise it will fail. Consult your database administrator or IT personnel for more information

Note: Server Configuration Tool can also be launched from the following location
C:\Program Files (x86)\First Access Express or C:\Program Files (x86)\First Access Advanced

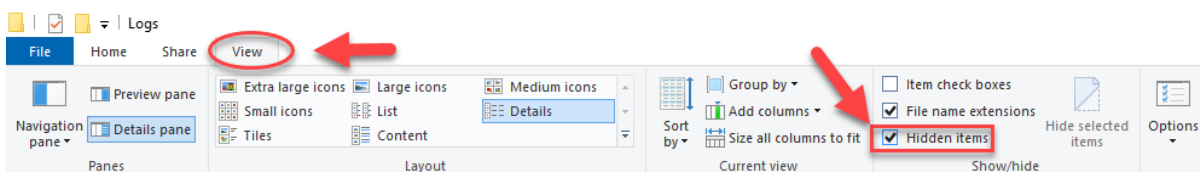


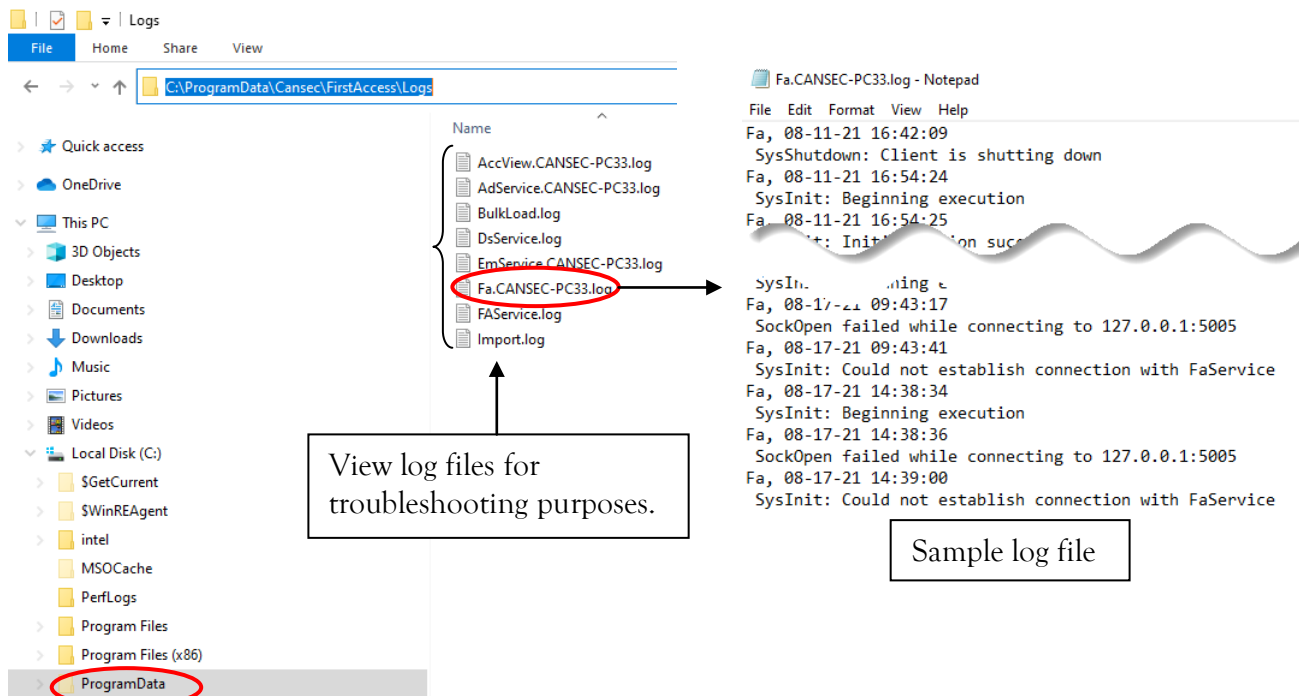
Select Build to build the connection string then select Test to test the connection. If successfully, select Save to save the connection string and otherwise consult your database administrator or IT personnel

- Fail to back up or restore the database is due to the improper login credential. Follow option 1 or 2 above to fix it before backup or restore can be done.

Note:

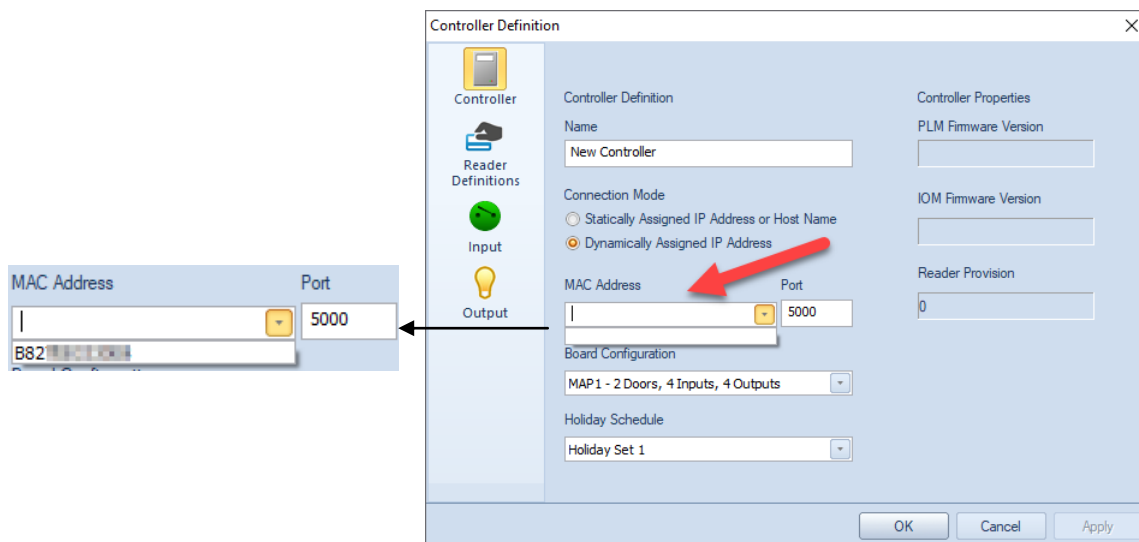
The logs files can be accessed and viewed from this location C:\ProgramData\Cansec\First Access\Logs. In Windows 10 ensure that you enable hidden items in order to view and access the C:\ProgramData folder which is hidden by default in Windows.



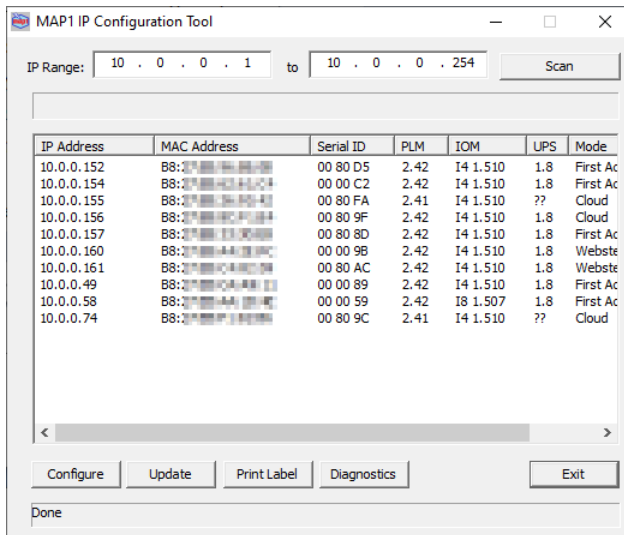


➤ No controllers found

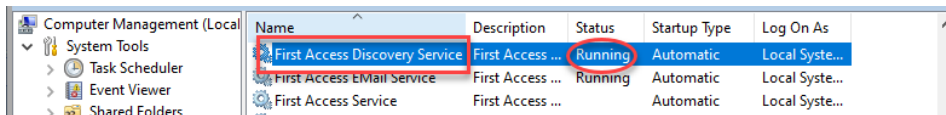
When adding a new controller the MAC address field shows an empty list. *Normally it should show at least one entry provided that the controller is powered on and connected to the same network with the computer hosting the First Access server.*



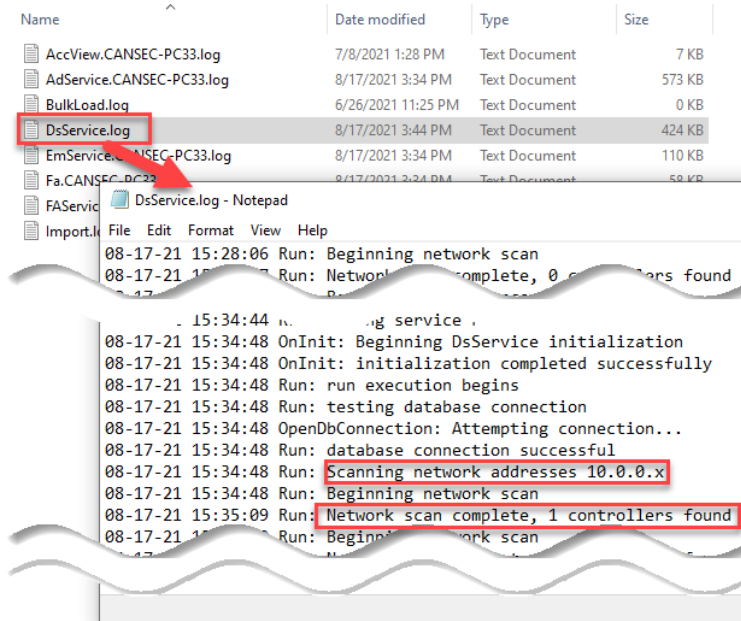
- Use the MAP1 IP Configuration Tool to scan for all controllers to ensure that they are at least detected by this standalone tool.



- Ensure that the First Access Discovery Service (DsService) is running.



- Check the log file to ensure that the DsService has found at least one controller.



- Ensure that the controllers and the computer hosting the First Access server are on the same network or subnet.

® First Access is a registered trademark of Cansec Systems Ltd.

® Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.